THE SHIFTING THREAT LANDSCAPE AND MOBILE DEVICE SECURITY

Leslie K. Lambert
Juniper Networks
VP & Chief Information Security Officer
July 16, 2011

AGENDA

Today's Shifting Threat Landscape

Mobile Device Security

TODAY'S SHIFTING THREAT LANDSCAPE

The Sophisticated Cybercriminal

- Cybercriminals - from students to well paid organized professionals
- Advanced Persistent Threats - Sophisticated and strategic efforts aimed at intelligence gathering and espionage

The Threat from Within

- Insiders with and without malicious intent
- The mobile device as Trojan Horse

CHANGE IN ‘ATTACKER BEHAVIOR’

Notoriety


The Daily

HACKERS TAKE DOWN MOST WIRED COUNTRY IN EUROPE

The minister of defense checked the Web page again — still nothing. He stared at the error message: For some reason, the site for Estonia's leading newspaper, the Postimees, wasn't responding. Jaak Aaviksoo attempted to pull up the sites of a couple of other papers. They were

Profitability

.gov /.com

.me / .you / .edu

SECURITY IS IMPACTED BY TWO TRENDS

Industry Trends

Mobile Workforce

Data Center Consolidation

Consumerization

Security Trends

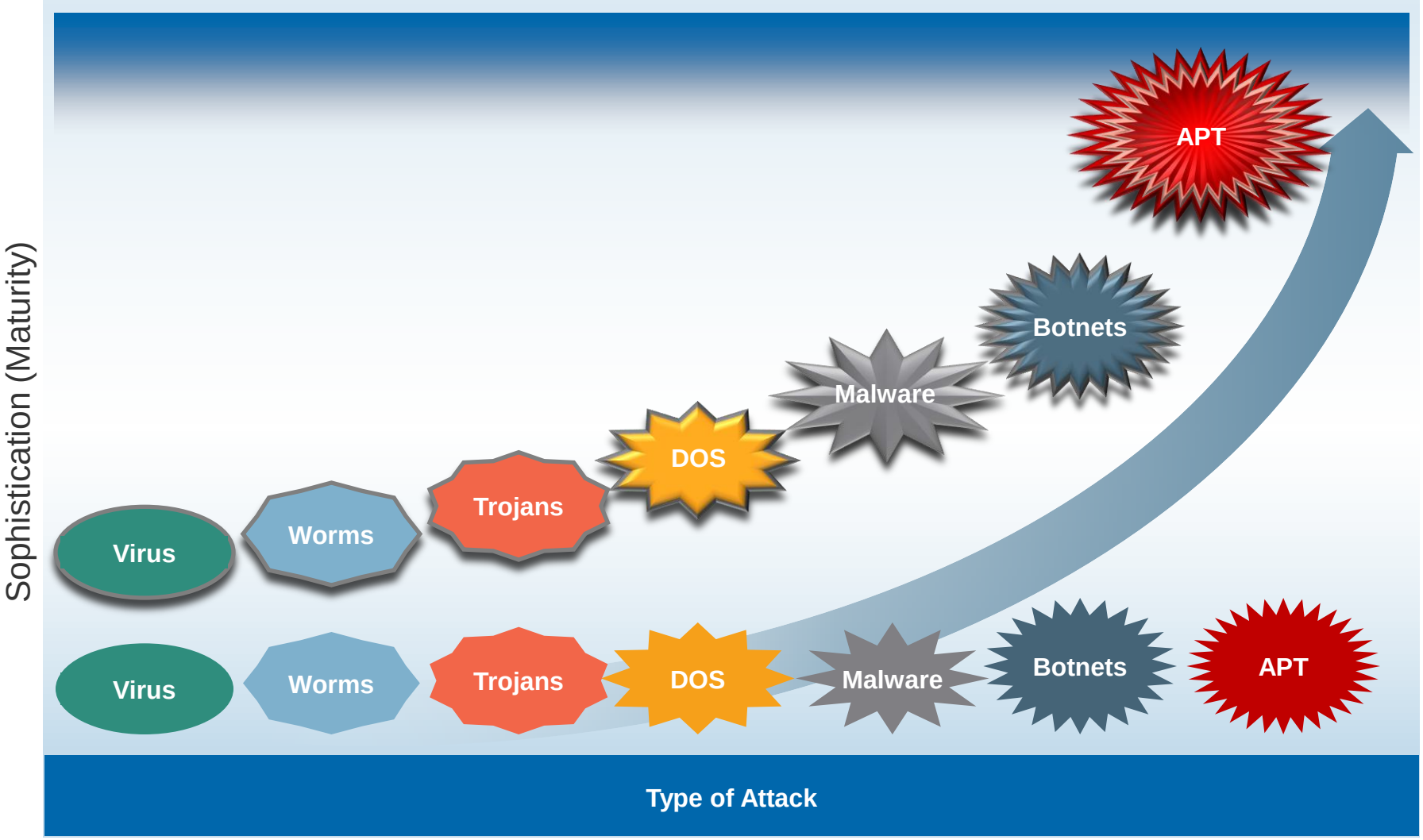
Evolving Threat Vectors

New Attack Targets

Attacker behavior

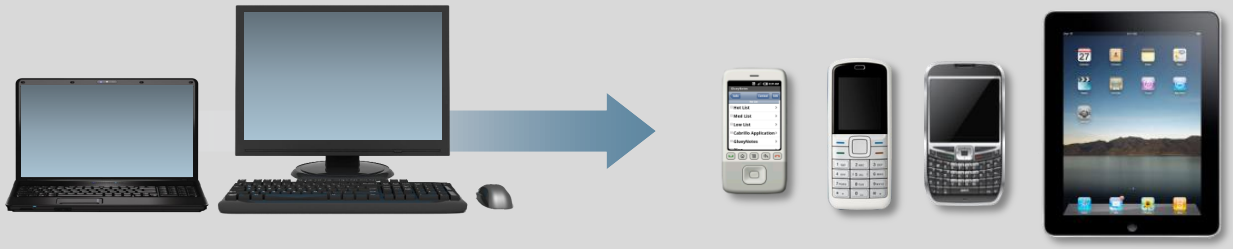
INDUSTRY TRENDS
CONSUMERIZATION OF IT

SECURITY TRENDS
EVOLVING THREAT VECTORS

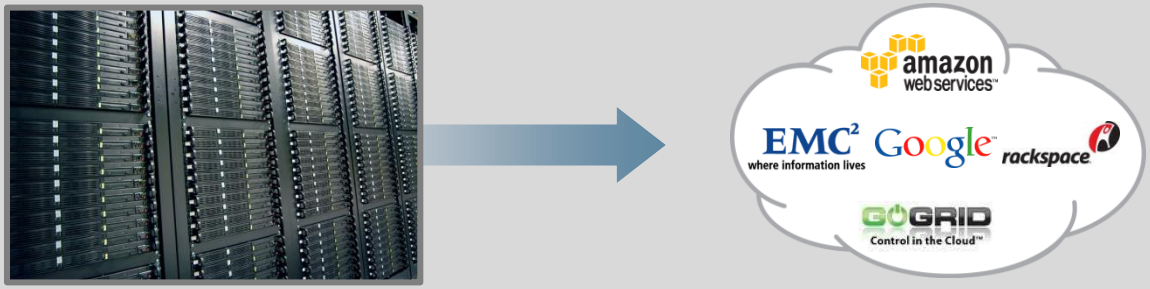


NEW TARGETS

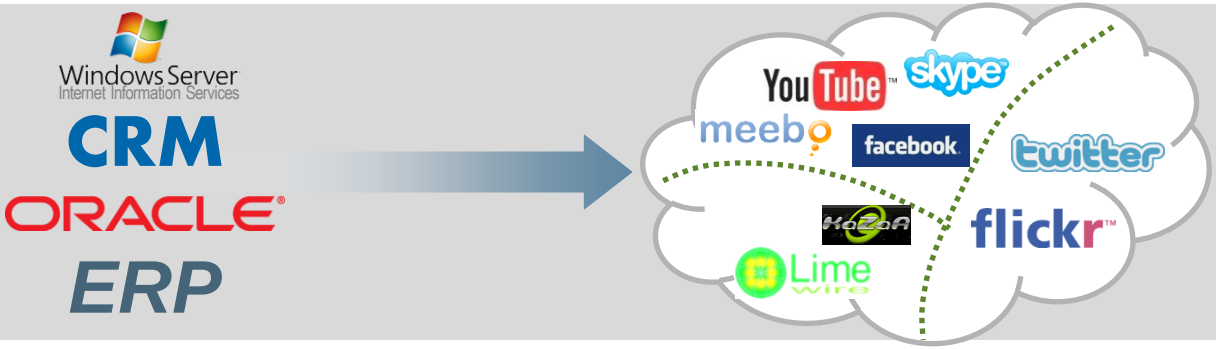
New Devices



New Cloud Services



New Applications



SECURITY'S EVOLVING AND EXPANDING BATTLEFRONTS

The Decentralized Nature of Attacks

Inadequate security on mobile devices

Diverse user profiles

Device and OS proliferation

Increasing implementation points

SECURITY'S EVOLVING AND EXPANDING BATTLEFRONTS

The Cloud and Web 2.0

Virtualization complexity

One Web, many uses

Clouds of uncertainty

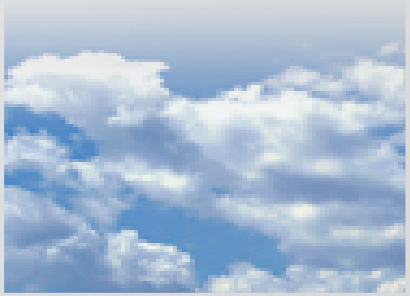
MANAGING NETWORKING AND SECURITY IN AN INTEGRATED FASHION

Security Function

View and Manage all Vital Security Functions

Accommodate New Security Services

Embrace Open Standards



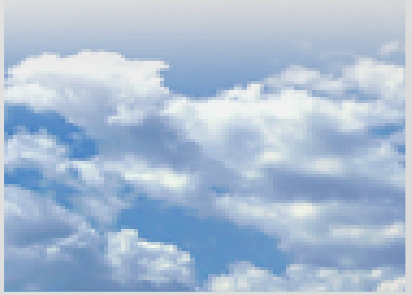
MANAGING NETWORKING AND SECURITY IN AN INTEGRATED FASHION

Multilayer Intelligence

Take a Cohesive, Centralized Approach

Enforce Application-Centric Security Policies

Identify Threats to the Virtual Infrastructure



MANAGING NETWORKING AND SECURITY IN AN INTEGRATED FASHION

Diverse OS and Device Type Support

Apply Security Across Broad Range of Devices

Device Security Integrated at the Server and Network Level

Manage Less Security on the Actual Device

JUNIPER NETWORKS

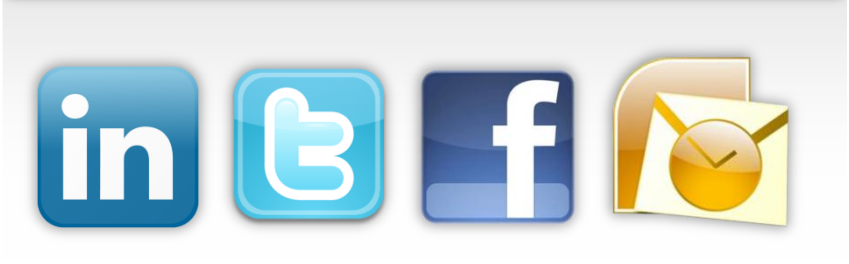
MOBILE DEVICE SECURITY: EMERGING THREATS, ESSENTIAL STRATEGIES

THE MOBILE INTERNET IS THE NEW INTERNET

Proliferation of Devices

Number of smartphones sales to exceed PC sales in 2012*

Connected Socialization



Content Consumption

*Source: Morgan Stanley, 2010

DEMANDS OF TODAY'S MOBILE USER

ANY Device

ANY Location

ANY Application

NEW RESEARCH REVEALS A GAP BETWEEN BEHAVIOR AND THE DESIRE TO BE SAFE

40%
use their smartphone for both personal and business

72%
share or access sensitive info such as banking, credit card, social security, medical records

80%
access their employer's network without permission
-- 59% **do it everyday**

50%+
are very concerned about loss, theft and identity theft resulting from their mobile usage

Sources: KRC Research and Juniper Mobile Threat Center

MALWARE HISTORY TELLS US TWO THINGS

1. Malware changes and gets more sophisticated

1966 — **Academic Foundation**
Theory of self-reproducing automata
John von Neumann, Institute for Advanced Study Site Y
Los Alamos

1981 — **Executable Boot Sector Infections**
Elk Cloner (Apple II) '81

1986 — **Executable Boot Sector Infections**
Brain Boot Sector (PC) '86

1995 — **Macro Viruses**
Concept '95
Melissa '99

2001 — **Network Worm**
Code Red '01
Nimda '01

2009 — **Mobile Malware**
SMS Trojan – '09
Symbian, July, '10 Android

'66 '81 '86 '95 '01 '09

'88 '90

1988 — **Fred Cohen**
"On the implications of Computer Viruses and Methods of Defense"

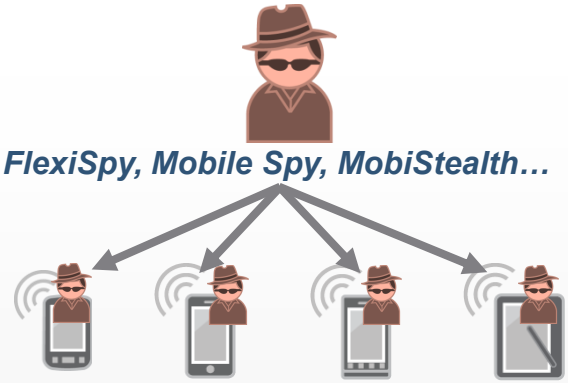
1990 — **Anti-Virus Firms**
20 + anti-virus firms

2. Waiting and reacting after-the-fact can be costly

EVOLUTION OF MOBILE MALWARE

Criminals now using PC-style malware attacks to infect mobile devices

Greatest mobile malware risk comes from rapid proliferation of applications in app stores



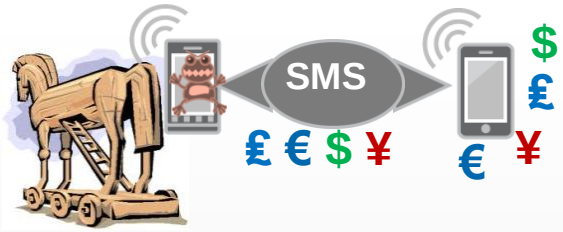
Mobile spyware is prevalent and now commercialized

2009 → **2010**

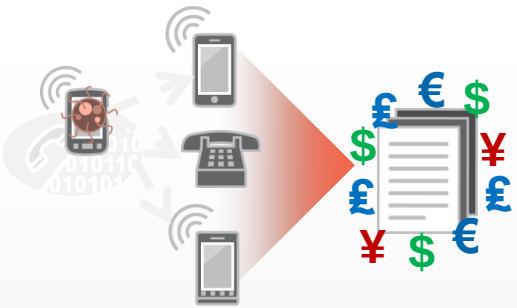
Between 2009 and 2010, reported increase in mobile threats of 250%*

*Information obtained from analysis of Junos Pulse Mobile Security Suite virus definition database dated 10/15/2010

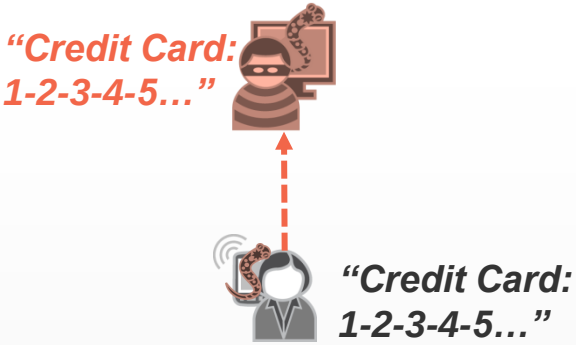
FAST PROLIFERATING MOBILE MALWARE THREATS



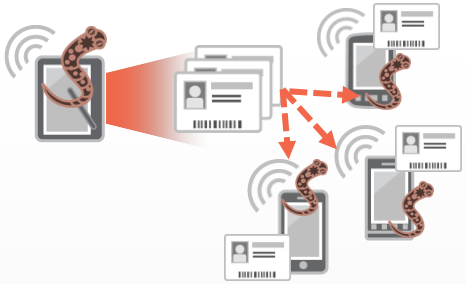
Trojans that send SMS messages to premium rate numbers



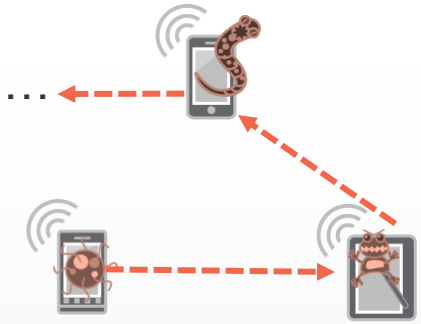
Background calling apps that rack up exorbitant long distance bills



Keylogging applications that compromise passwords and credit card or bank account numbers



Self-propagating code that infects devices and spreads to additional devices listed in a user's address book



Malware growing more sophisticated, now with polymorphic attacks

MOBILE DEVICE LOSS AND THEFT

A survey of consumer users found that one out of every three users lost their mobile device[1]

Approximately 2 million smartphones were stolen in the U.S. in 2008[2]

Over 56,000 mobile devices were left in the back seats of the city of London taxi cabs during a 6-month period between 2008 and 2009

Over the 2010 holidays, in the U.K. alone, a total of 5,100 smartphones and 3,844 notebook computers were lost at 15 different airports[3]

In Paris, 75% of 991 violent crimes that took place in October 2010 happened because of mobile phone theft[4]

[1]Information obtained from Junos Pulse Mobile Security Suite internal transaction logs; [2]Forrester Research; [3]Credant Technologies; [4]The Sydney Morning Herald, 12/10/10

WHY IS MOBILE DEVICE LOSS AND THEFT AN ISSUE?

Bookmarked bank accounts with passwords set to auto-complete

Contacts with pictures and addresses tied to the contact

Pre-connected personal data compilation sites

Social media accounts

Calendar events

Personal photos

YAHOO!

Pre-connected e-mail accounts

Sensitive corporate data and IP

JUNIPER NETWORKS

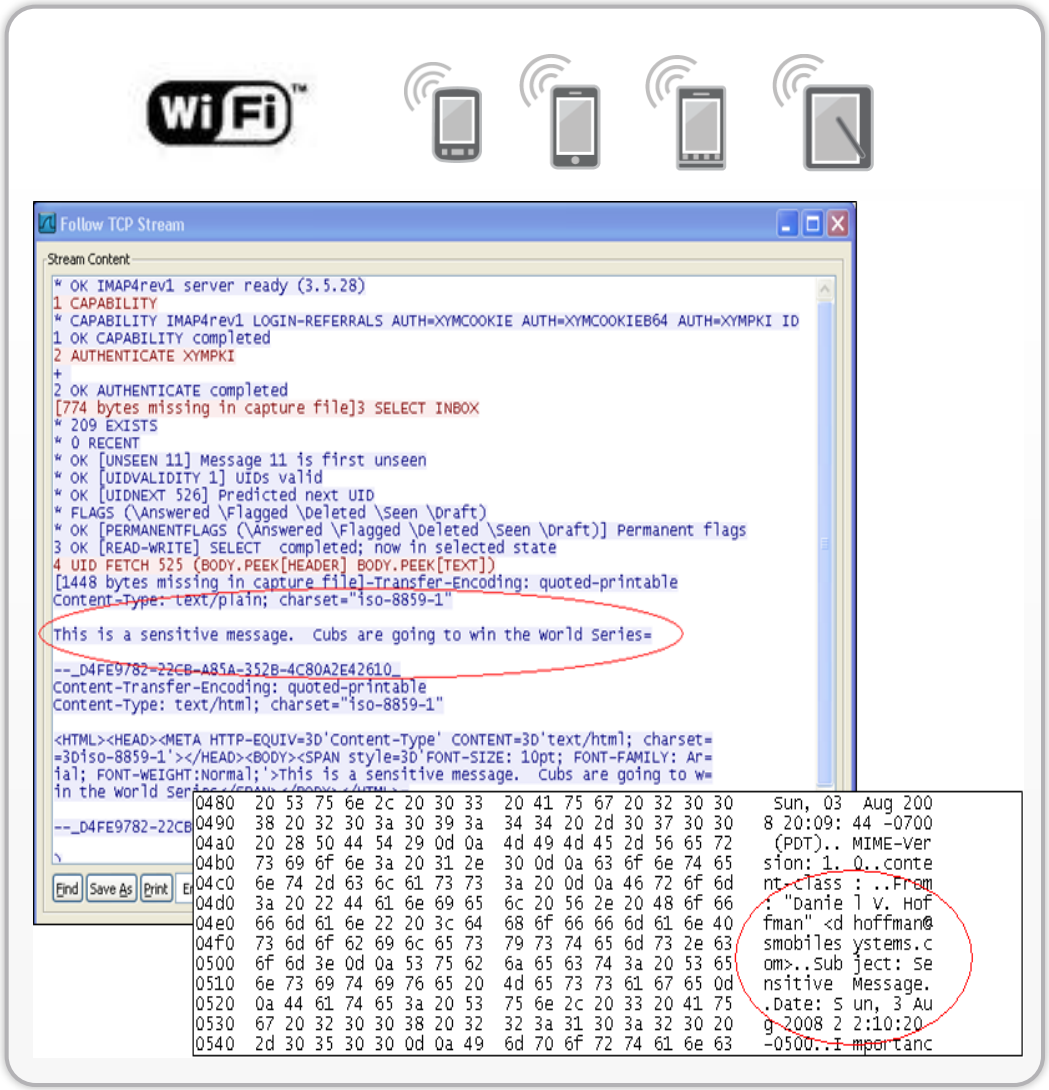
COMMUNICATION INTERCEPTION

Approximately 50% of all smartphones today are Wi-Fi capable[5]

Estimated 90% of all mobile devices will be Wi-Fi capable by 2014[5]

Risk of Wi-Fi sniffing and interception increases as number of Wi-Fi capable mobile devices increase

Once mobile device switches to a Wi-Fi network, it is susceptible to man-in-the-middle (MITM) attacks[6]



[5]http://www.wi-fi.org/news_articles.php?f=media_news&news_id=969;
[6]http://threatcenter.smobilesystems.com/?p=1587

MINIMUM REQUIREMENTS FOR ADDRESSING TODAY'S MOBILE THREATS

Proactive malware protection

- Protect mobile devices against malware and viruses delivered via any transmission means
- Frequent virus definition updates
- Real-time scanning of incoming files
- Scan of internal memory, memory cards, and entire device with ability to generate automated alerts

Loss and theft protection

- Integrated mobile device management capabilities
- Use GPS to identify the location of missing device
- Restore data to any subsequent device, regardless of mobile OS
- Remotely control devices, including initiating backups, locking, and data wiping

MINIMUM REQUIREMENTS FOR ADDRESSING TODAY'S MOBILE THREATS *(CONTINUED)*

Safeguards against communication interception

- Employ VPN that encrypts communications between mobile devices and corporate networks
- Establish and enforce corporate mobility policies
- Disable infected mobile device access

Device monitoring capabilities

- Protect children from cyberbullying and sexting
- Alert parents in the event such behavior occurs

ADDITIONAL CONSIDERATION FOR ADDRESSING TODAY'S MOBILE THREATS

Broad Device and Mobile OS Support

- Smartphones, tablets, netbooks, and notebooks are complementary in nature
- Need to account for a broad set of devices
- Same type of multi-factor authentication should be supported on all devices

Integrated Mobile Device Management (MDM) and Security Policy Enforcement

- Centralized control of disparate mobile device platforms and types
- Cohesive MDM and security policy enforcement
- Enforce granular, role-based access control to corporate applications
- Deliver seamless, cross-platform authentication for all users, regardless of device

Minimize End User Requirements

Leverage Self-Help Models to Reduce Overhead

THE GOAL → SECURE & SCALABLE MOBILITY

Mobile device threats are pervasive and escalating

Malware, loss and theft, exploitation and misconduct, communication interception, and direct attacks

With Juniper's JUNOS Pulse, enterprises and users can cost effectively guard against current and emerging threats while retaining optimal productivity and flexibility in mobile device use

- Scalable VPN infrastructure (with choice of physical or virtual appliances)
- Scalable Mobile Security infrastructure (with secure, hosted deployment)
- Broad range of mobile platform support covering all leading mobile platforms

everywhere