AT&T Mobile Security
Advanced Protection Throughout Your Network

July 2012

Rethink Possible®

Why consider mobile security?

The Risk

Personal mobile devices connected to the enterprise have brought new options to employees while simultaneously broadening the number and types of devices accessing your corporate network, and putting your sensitive data, processes, and tools at risk

Security Risks of an Unprotected Mobile Inventory

- Data Loss

- Mobile Threats

- Legal, Regulatory and Compliance Risks

Mobile Security Challenges

Malware
Viruses, Worms, Trojans, Spyware

Loss and Theft
Loss or inappropriate access of sensitive data

Data Communication Interception
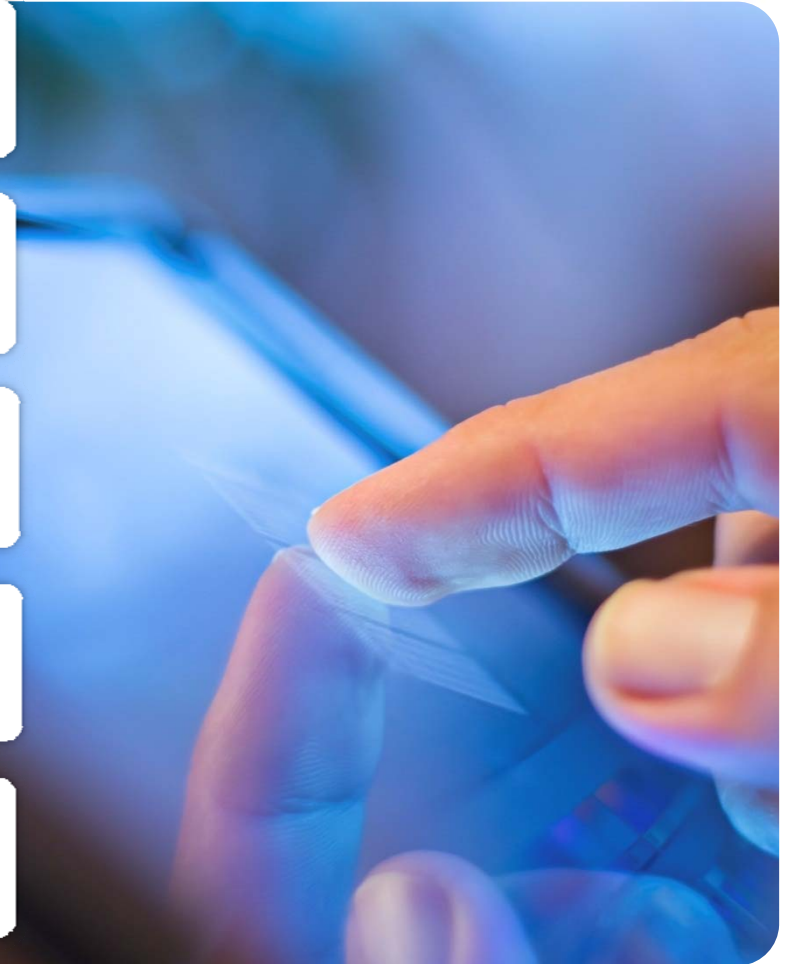Sniffing data as it is transmitted and received

Exploitation and Misconduct
Online predators, inappropriate sites and communications, data leakage

Direct Attacks
Attacking device interfaces, Network DoS, Malicious SMS

Business Challenges

Smartphone user behavior and expectations

89%
Business users accessing critical work data from their personal mobile device[1]

1.19 BILLION
Worldwide mobile worker population by end of 2013[2]

41%
Business users using personal device for work without company permission/knowledge[1]

35%
World's workforce expected to be mobile by end of 2013[2]

30%
IT pros whose company has experienced security threat due to a personal mobile device[1]

32%
IT Pros concerned personal mobile devices introducing malware[1]

41%
IT pros concerned about security breaches due to lost or stolen mobile devices[1]

155%
Mobile Malware increase from 2010 to 2011[3]

SOURCE:
[1] Juniper Networks' Trusted Mobility Index
[2] IDC
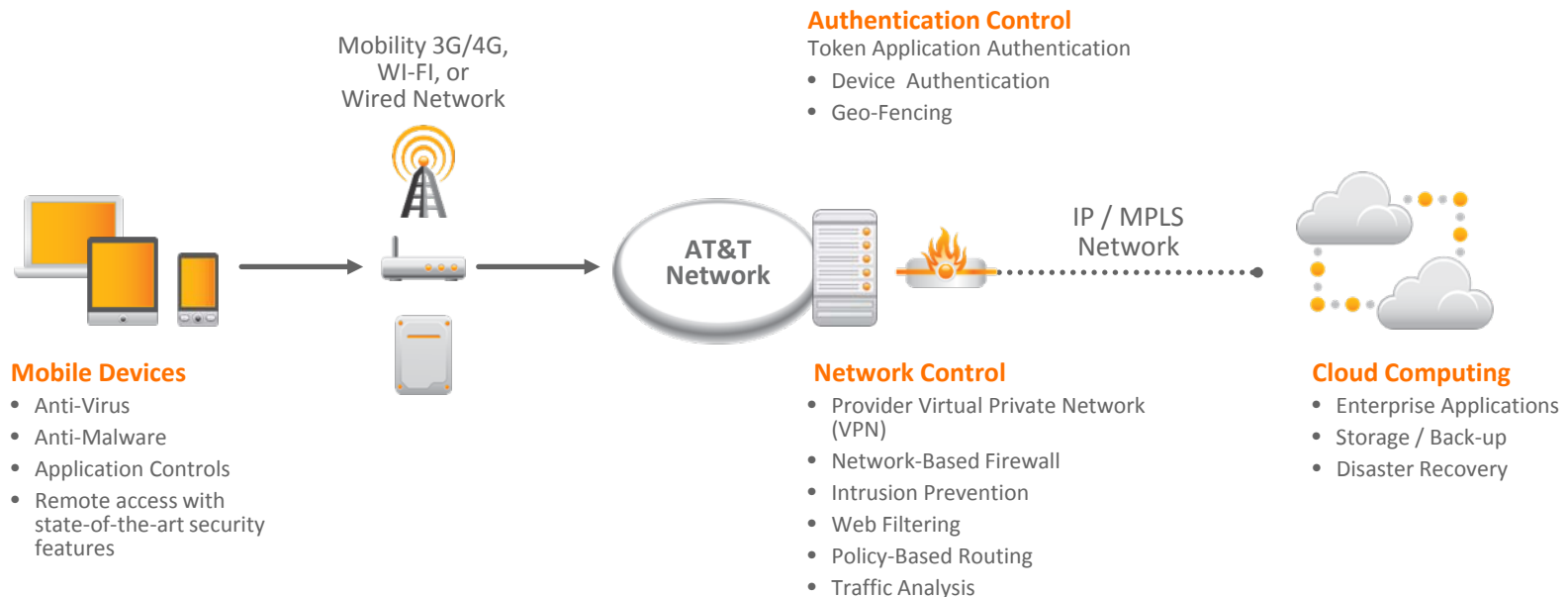[3] Juniper Networks' 2011 Mobile Threat Report

AT&T Mobile Security Solution

Deploy an application on mobile devices that includes network-based, carrier-grade protection (Carrier Agnostic)

- Downloads to the mobile device to help protect its connection to the Internet providing multi-layer security and device management capabilities

- Integrates device-level security features with network-based security controls and encrypted transport for a comprehensive solution

- Botnet, Anti-virus, Anti-malware, Malicious Application mitigation to help enforce your security policies

Mobility 3G/4G, WI-FI, or Wired Network

Authentication Control
Token Application Authentication
- Device Authentication
- Geo-Fencing

AT&T Network

IP / MPLS Network

Mobile Devices
- Anti-Virus
- Anti-Malware
- Application Controls
- Remote access with state-of-the-art security features

Network Control
- Provider Virtual Private Network (VPN)
- Network-Based Firewall
- Intrusion Prevention
- Web Filtering
- Policy-Based Routing
- Traffic Analysis

Cloud Computing
- Enterprise Applications
- Storage / Back-up
- Disaster Recovery

AT&T Mobile Security

Features

- Anti-virus, Anti-malware , Malicious application mitigation
- Root/Jailbreak detection
- Scans files received over network connections
- Network-Based Firewall monitors Inbound , outbound traffic
- BotNet Black list and White list filtering
- Network Security Controls
- Loss or theft protection
- Customer Administrative Portal

Benefits

- Real time virus, malware, malicious application protection
- Detects rooted or "jailbroken" devices, prohibits connection to the network
- Helps protect from threats delivered via SMS, MMS, Bluetooth, Wi-Fi, 2.5G, 3G, 4G, infrared or desktop sync
- Safe guards device from accessing harmful content, prevents malicious content from transferring to the device
- Blocks device from accessing known malicious sites, and permits access to clean sites
- Extends wireline network security policies to wireless endpoints; Connectivity to AT&T Remote Access Services, AT&T VPN services, and AT&T Secure Network Gateway for added security
- Remotely locates & locks and wipes the device contents
- Enables device management, registration and control over your security policy from a central location

Mobile Security helps you….

Provide key features to address security concerns

- Extend, help protect and synchronize security controls and policies across wireline and wireless environments to ease compliance

- Helps protect network and mobile devices with anti-virus and anti-malware

- Identify and block botnets

- Restrict mobile access to unauthorized sites

- Administrator controls security policies in the network, with AT&T managing the infrastructure, licenses, patches and support