+44 20 8123 2220
info@marketpublishers.com

The Mobile Device & Network Security Bible: 2013 - 2020

https://marketpublishers.com/r/MAB5F402FE5EN.html
Date: September 2013
Pages: 284
Price: US$ 2,500.00 (Single User License)
ID: MAB5F402FE5EN

Abstracts

Mobile networks around the globe generate more than 50 Exabytes of traffic annually. The immense volume of traffic together with the growing adoption of open source Operating System (OS) platforms such as Android has opened up new security threats. Mobile malware, SMS spam, cyber attacks and unlawful eavesdropping are an ever-increasing problem for enterprises, consumers and mobile network operators around the globe.

This has in turn led to significant investments in integrated security appliances and content security gateways by both enterprises and mobile network operators, besides opening doors for emerging submarkets such as mobile Security as a Service (SEaaS).

On the devices front, installation of Anti-Malware/Anti-Virus client software is fast becoming a de-facto requirement for most smartphones and tablets. Furthermore, mobile device OEMs are also integrating advanced biometrics such as fingerprint sensing into their smartphones and tablets, amid growing popularity of security sensitive opportunities such as mobile payments.

Driven by the thriving ecosystem, SNS Research estimates that mobile device and network security investments will account for nearly $9 Billion in 2013 alone. The market is further expected to grow at a CAGR of nearly 21% over the next 7 years.

This report presents in-depth assessment of the global mobile device and network security market, and covers four individual submarkets. In addition to covering key market drivers, challenges, future roadmap, value chain analysis, deployment case studies and vendor service/product strategies for each submarket, the report also presents comprehensive forecasts for the mobile device and network security market

+44 20 8123 2220
info@marketpublishers.com

from 2013 till 2020. Historical revenue figures for 2010 – 2012 are also presented. The forecasts and historical revenue figures are individually segmented for four submarkets, 17 product/service categories, six geographical regions and 34 countries.

The report comes with an associated Excel datasheet covering quantitative data from all figures presented within the report.

Topics Covered:

The report covers the following topics:

- An in-depth analysis for four individual submarkets and their associated product/service categories: Mobile Network Infrastructure Security Software & Appliances, Mobile Device Client Security Software, Mobile Device Security Hardware and Mobile Security & MDM Services
- Value chain analysis for each submarket
- Key market drivers and challenges for each submarket
- Key trends for each submarket
- Case studies on product/service deployment for each submarket
- Profiles and strategies of key players in the market
- Historical revenue figures and forecasts till 2020

Historical Revenue & Forecast Segmentation:

Market forecasts and historical revenue figures are provided for each of the following submarkets and their 17 product/service categories:

- Mobile Network Infrastructure Security Software & Appliances
  - Integrated Security Appliances (Hardware & Software)

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

The following regional and country markets are also covered:

Regional Markets

Asia Pacific

Eastern Europe

Latin & Central America

Middle East & Africa

North America

Western Europe

Country Markets

Argentina, Australia, Brazil, Canada, China, Czech Republic, Denmark, Finland, France, Germany, India, Indonesia, Israel, Italy, Japan, Malaysia, Mexico, Norway, Pakistan, Philippines, Poland, Qatar, Russia, Saudi Arabia, Singapore, South Africa, South Korea, Spain, Sweden, Taiwan, Thailand, UAE, UK, USA**Key Findings:**

The report has the following key findings:

Driven by the thriving ecosystem, SNS Research estimates that mobile device and network security investments will account for nearly $9 Billion in 2013 alone. The market is further expected to grow at a CAGR of nearly 21% over the next 7 years

Enterprises and mobile network operators have made significant investments in integrated security appliances and content security gateways (including those specific to SMS/MMS security)

The installation of Anti-Malware/Anti-Virus client software is fast becoming a de-facto requirement for most smartphones and tablets

More than half of all enterprises allow the use of employed owned mobile

+44 20 8123 2220
info@marketpublishers.com

devices on their networks. Enterprises thus continue to aggressively adopt SSL VPNs in their mobile security strategies to ensure connection security in addition to activity monitoring and control

Mobile Device Management (MDM) services providers are eyeing on opportunities for cloud based mobile security services that extend existing security policies to enterprise mobile devices to help secure data, reduce risk and protect the enterprise, which has created a new submarket for mobile Security as a Service (SEaaS)

Key Questions Answered:

The report provides answers to the following key questions:

How big is the mobile device and network security market, and what particular submarkets does it constitute?

Who are the key players in each submarket?

How is the value chain structured for each submarket and how will it evolve overtime?

Which regions and countries will witness the highest percentage of growth in mobile security spending?

Will recent privacy scandals have a negative impact on mobile security spending in the coming years?

What known malware families are most dangerous for modern smartphones?

+44 20 8123 2220
info@marketpublishers.com

Contents

+44 20 8123 2220
info@marketpublishers.com

3 CHAPTER 3: MOBILE NETWORK INFRASTRUCTURE SECURITY SOFTWARE & APPLIANCES

+44 20 8123 2220
info@marketpublishers.com

4 CHAPTER 4: MOBILE DEVICE CLIENT SECURITY SOFTWARE

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

7 CHAPTER 7: KEY COMPANY PROFILES

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

8 CHAPTER 8: MARKET ANALYSIS & FORECASTS

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

List Of Figures

LIST OF FIGURES

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

+44 20 8123 2220
info@marketpublishers.com

About

SNS Research estimates that by the end of 2013, annual shipments of connected mobile devices will outnumber PC and notebook shipments by almost 1.6 Billion units.

The quantum jumps in connection speeds offered by mobile network operators have expanded the scope of content that can be rendered and exchanged using mobile devices, considerably. In 2013 alone, SNS Research estimates that mobile devices will generate nearly 58 Exabyte's of network traffic.

Anti-Malware/Anti-Virus Client Software

Mobile anti-virus works pretty much like its PC counterpart. Antivirus protects devices against viruses and other malicious programs such as Trojans, rootkits, worms, spyware and others.

Detection Mechanism: How it Works?

Anti-virus technology, at its heart, is a detection tool. Anti-viruses look for signatures of known viruses, predominantly in code that can be executed. Their work does not stop with that, as they have to detect unknown threats as well. These are instances of malicious code that have not been identified. Here, they employ heuristic techniques, which combine anomaly detection with specific instances of behavior of known viruses to checkmate impending threats. Present day anti-viruses do not limit themselves to scanning resources only on being prompted; they form a veritable protective shield which keeps an eye on critical system resources to detect the presence of malicious code. The shield helps in achieving real time protection for the device.

Delivery Mode

Mobile anti-viruses can be downloaded directly on mobile devices through the vendor's website or the application market place run by the mobile OS developer. In earlier years, the preferred mode of mobile antivirus installation was to transfer it to the device from a PC.

MHz band. This is an unlicensed band reserved for industrial, scientific and medical (ISM) applications. Maximum data rate supported by NFC are 424 kbps. Clearly, NFC is a low data rate standard. Its operating range distance is capped typically at 10 cm.

+44 20 8123 2220
info@marketpublishers.com

While a majority of the NFC use-cases are in the form of readertag communication; peer-to-peer communication is also possible, provided both the devices are powered. NFC is supposed to be in active mode if the tags have access to power independently. In such cases, the tag and the reader can generate their own magnetic fields. When independent power to the tag is absent, NFC is said to be acting in a passive mode, wherein the tag works by modulating the field generated by the reader by drawing power from the reader device.

Is NFC Immune to Eavesdropping?

As NFC works on the principle of proximity, it is thought of being inherently secure. It is practically very difficult for hackers to intercept communication from such close quarters. However, this belief could be misleading as NFC is not entirely immune to eavesdropping, although the eavesdropper has to be in close proximity of the NFC enabled handset. Also, passive NFC tags are believed to be less susceptible to being eavesdropped as compared to their active counterparts. The potency of the eavesdropping threat is determined by antenna geometry of the eavesdropper as well as the target, distance between the eavesdropper and the target, as well as by the signal quality available to the eavesdropper. Philips, one of the developers of NFC also enlists data corruption, insertion and modification as less probable, but theoretically possible, vulnerabilities of NFC devices.

Key Players in the Market

Vendor landscape is the most accurate barometer of the market potential of a technology. On this count, mobile biometrics is on a sound footing. Considering that it is very much in the fledgling stage, it enjoys considerable interest, as evidenced in the significant number of companies foraying into it. Some of the salient participants are highlighted below:

- 3M Cogent supplies finger print and facial recognition systems for law enforcement, as well as commercial domains.
- Inside Secure provides modular solutions for fingerprint as well as swipebased authentication.
- Bayometric makes mobile fingerprint scanners that are present as a hardware attachment.

+44 20 8123 2220
info@marketpublishers.com

- Cross Match Technologies provides multimodal biometric mobile solutions, predominantly to the law enforcement agencies.

- CrucialTec's mobile fingerprint scanners are embedded in the home button itself; making authentication intuitive and convenient.

- Fulcrum Biometerics provides multimodal biometric applications for Android as well as iOS, including face, iris and fingerprint

- Iris ID is a pioneer in the development of a combined iris and facial recognition system.

+44 20 8123 2220
info@marketpublishers.com

I would like to order

Product name: The Mobile Device & Network Security Bible: 2013 - 2020

Product link: https://marketpublishers.com/r/MAB5F402FE5EN.html

Price: US$ 2,500.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/MAB5F402FE5EN.html