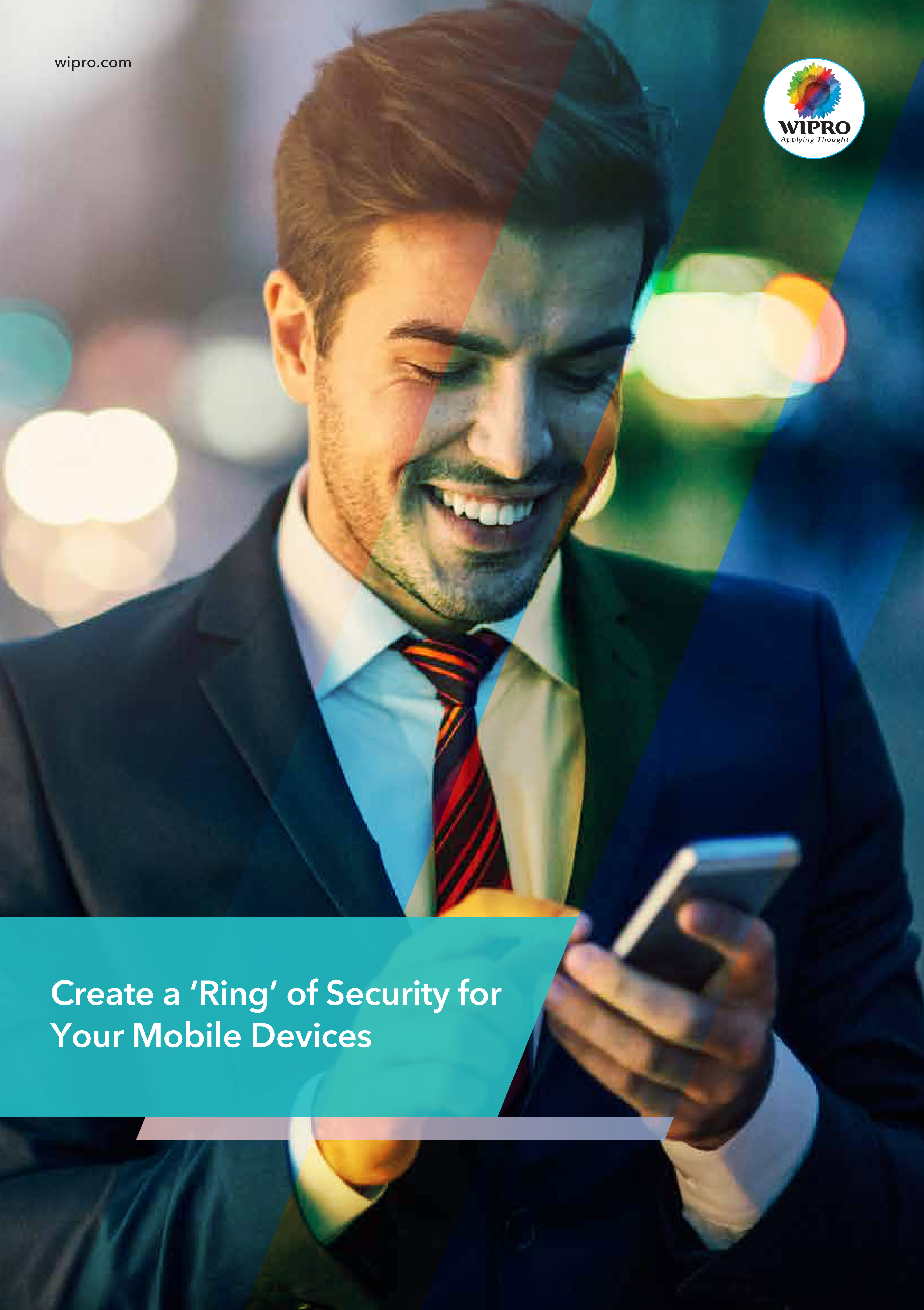
wipro.com



Create a 'Ring' of Security for Your Mobile Devices

Mobile devices dominate our lives. Personal (BYOD) and enterprise-owned mobile devices are now permeating every part of the enterprise. Globalization, affordability and convenience of mobile devices, and the anywhere anytime work culture of millennials, are fueling this adoption. Industry forecasts show that the global mobile workforce will grow from more than 35% in 2014 to over 40% by 2020. Simultaneously, types of mobile devices are on the increase: mobile POS devices, scanners, smart phones, tablets, wearables, VR headsets and function-specific Heads Up Displays (HUD) are just a few. To this, add the growing number of applications running on these devices (Google Play alone had 2.2 million apps as of mid-2016[i]) and you can see why mobile technology is transforming the world.

But there is a dark side to the trend. The surge in mobile adoption presents new challenges to enterprises in securing their information. The numbers behind the trend provide a clue to the enormity of the threat. A recent estimate by mobile security researchers and specialists put the average cost of mobile data breaches in excess of $25 million for large enterprises. The same study found that about 3% of employee devices were infected with malware and about 70% of organizations reported data breaches as employees used mobile devices to access sensitive and confidential data.

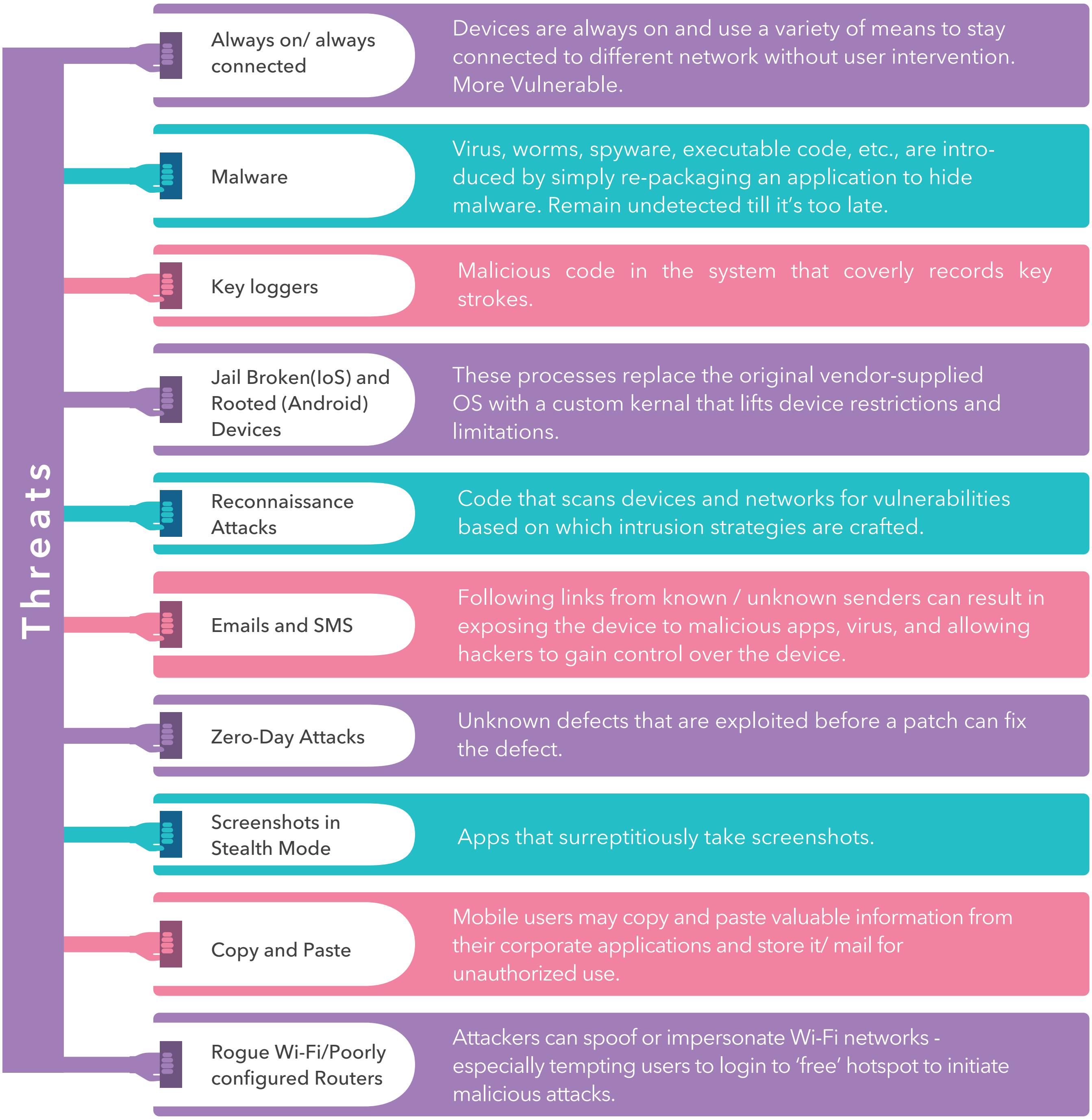
It is obvious then that while Enterprise Mobility Management (EMM) and Mobile Device Management (MDM) solutions are essential, they are currently not equipped to handle emerging security needs.

[i] http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

Ever-changing nature of threats

The risks to mobile users and enterprise information are getting truly complex. Traditional threat management – the use of anti-virus, for example that looks for known patterns – is no longer adequate to deter hackers and malicious attackers. The need is to detect known and unknown (zero-day) threats in real time and provide users with immediate remedial action/s. This means 24X7 surveillance of apps, networks and user behavior to detect threats.

Enterprises need to create a comprehensive solution that addresses threats resulting from (see Figure 1)



Threats

Always on/ always connected: Devices are always on and use a variety of means to stay connected to different network without user intervention. More Vulnerable.

Malware: Virus, worms, spyware, executable code, etc., are introduced by simply re-packaging an application to hide malware. Remain undetected till it's too late.

Key loggers: Malicious code in the system that coverly records key strokes.

Jail Broken(IoS) and Rooted (Android) Devices: These processes replace the original vendor-supplied OS with a custom kernal that lifts device restrictions and limitations.

Reconnaissance Attacks: Code that scans devices and networks for vulnerabilities based on which intrusion strategies are crafted.

Emails and SMS: Following links from known / unknown senders can result in exposing the device to malicious apps, virus, and allowing hackers to gain control over the device.

Zero-Day Attacks: Unknown defects that are exploited before a patch can fix the defect.

Screenshots in Stealth Mode: Apps that surreptitiously take screenshots.

Copy and Paste: Mobile users may copy and paste valuable information from their corporate applications and store it/ mail for unauthorized use.

Rogue Wi-Fi/Poorly configured Routers: Attackers can spoof or impersonate Wi-Fi networks - especially tempting users to login to 'free' hotspot to initiate malicious attacks.

Fig 1: Common Mobile Computing Threats

24x7 Vulnerability demands real-time response

Mobile devices are meant to remain always on and, by default, configured to stay connected (unlike, say, a laptop or a desktop). These devices use a variety of means to stay connected to different networks without user intervention. They are, therefore, highly vulnerable 24X7, and often without the knowledge of the user.

The always-on, 24X7 connected nature of mobile devices demands that no time can be lost in identifying intrusions and attacks – and taking immediate remedial action. Depending on the nature of the attack and risk involved, security measures should be configured to respond in real time, with or without the users consent across managed and unmanaged devices

Here are some of the areas enterprises can explore to strengthen their mobile security:

Firm up Mobile Security Policy – Put in place a mobile security policy that helps protect corporate data. Define various platform-supported guidelines for achieving confidentiality, integrity and availability (CIA triad) of corporate data. This is with regard to mobility, secure apps development and usage, operations and maintenance, as well as mobile device configuration.

Bolster Mobile Threat Management – Select Mobile Threat Management (MTM) solutions that meet the organization's mobile security policy. The MTM solution should be able to detect known and zero-day threats by monitoring apps, network, OS state and user behavior. Upon detection of a threat, it should also have the ability to respond/notify by not allowing users to perform further activity on the mobile device until malicious conditions are removed.

Strengthen Mobile Defense – Configure the MTM solution to immediately alert the cyber defense group about the mobile threat and associated critical information. Based on threat input received from the MTM solution, the organization can leverage on the cyber defense group's analytics solutions to achieve visibility into attacks/risks. For example, user behavior related gaps, geo-specific patterns, network-specific issues, applications and OS related vulnerabilities, etc.

Plan Effective App Security for BYOD Users - It is not always possible to enforce enterprise mobile security policies for third-party vendors, end customers or BYOD users.

Enterprises need to develop self-immune secure apps by adhering to OWASP M1-M10 risks and 91 OWASP mobile checklist. They need to plan incident response like notifying the cyber defense group and/or not allow corporate apps to boot until the threat is removed.

Looking beyond EMM

Mobile technology is advancing very rapidly. So is the threat it presents to an enterprise. Organizations must, in addition to the use of MDM and EMM, put in place security measures that effectively identify and respond to the growing number of threats in real time. Selecting an optimal security solution for an enterprise mobile environment can be tricky. It is easy to go to either extreme: underestimate or overestimate the threat. It is, therefore, necessary to have a thorough understanding of the business needs, technology environment, applications and compliance issues before narrowing down on a mobile security solution.

About the authors

Bhaveshkumar Bhatt currently leads the Cloud and Mobile Security Services in Wipro. He is responsible for thought leadership, solution strategy and transformation. With over 15 years of experience in the IT industry, Bhavesh has an expertise in Enterprise Security domain. He is adept at handling infrastructure, analytics, mobile, data security solution design and service delivery management across industry verticals.

He can be reached at **bhaveshkumar.bhatt1@wipro.com**

Mohammed Zakaullah has over 11 years of experience in the IT industry, of which 8 years has been in areas of Mobility. As a Lead Consultant in Wipro's Mobility business, he provides subject matter expertise in Enterprise Mobility for engagements across industry segments. He has experience in implementing Mobility Solutions for enterprises in B2B, B2C and B2E domains.

He can be reached at **mohammed.zakaullah@wipro.com**

About Wipro

Wipro Ltd. (NYSE:WIT) is a leading information technology, consulting and business process services company that delivers solutions to enable its clients do business better. Wipro delivers winning business outcomes through its deep industry experience and a 360 degree view of "Business through Technology." By combining digital strategy, customer centric design, advanced analytics and product engineering approach, Wipro helps its clients create successful and adaptive businesses. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, Wipro has a dedicated workforce of over 160,000, serving clients in 175+ cities across 6 continents. For more information, please visit **wipro.com** or write to us at **info@wipro.com**

DO BUSINESS BETTER

CONSULTING | SYSTEM INTEGRATION | BUSINESS PROCESS SERVICES

WIPRO TECHNOLOGIES, DODDAKANNELLI, SARJAPUR ROAD, BANGALORE - 560 035, INDIA. TEL : +91 (80) 2844 0011, FAX : +91 (80) 2844 0256

IND/B&T/JAN-DEC2016