MOBILE CYBERSECURITY IN THE DIGITAL ECONOMY

9 September 2016

Lookout

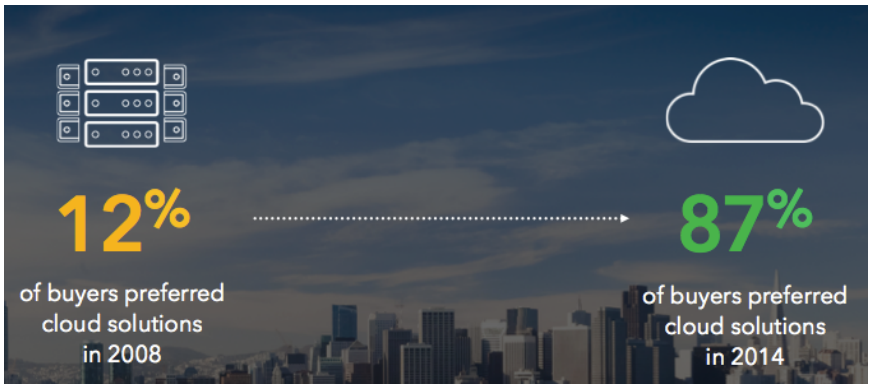
Modern organizations have recognized the need to embrace mobile devices and the benefits they can provide in the workplace. However, when it comes to Cybersecurity for mobile devices, most IT and security professionals have overlooked this important aspect of their environment. The thinking is that the biggest security challenges were on PCs, where employees did the majority of their work. As cloud-based services proliferate and more mobile applications are increasingly available for businesses, the vast majority of employees now rely on mobile devices for productivity, forcing IT departments to rethink device security priorities to include mobile. Mobile devices are increasingly becoming the primary method to access corporate data and resources so security professionals need to develop strategies for securing their mobile environment

The mobile, demanding, and productive workforce is literally dragging companies into this new world. The way we work, live and connect is different, and over the next few years we will see a complete transformation in the way security is used to protect people and businesses where mobility and cloud access to data are requirements. We think the world is mobile today, but in fact, we're just scratching the surface.

Gartner estimates that there will be 5.3B smartphones and tablets in 2019. To give that number context: the world population to be 7.5B people by that time. Nearly every person on earth will have a smartphone or tablet by then. In Mary Meeker's latest "State of the Internet" report, it found that time spent on mobile surpassed desktops in 2014. That number went up even further to 51% in 2015.

Operating systems and form factors are also converging as new productivity tools are coming to market. The iPad Pro is practically a laptop itself with the content creation capabilities that come with a keyboard. Windows 10 is the first operating system to serve all form factors, but doubtfully the last. The world has gone mobile and the way you secure it needs to as well.

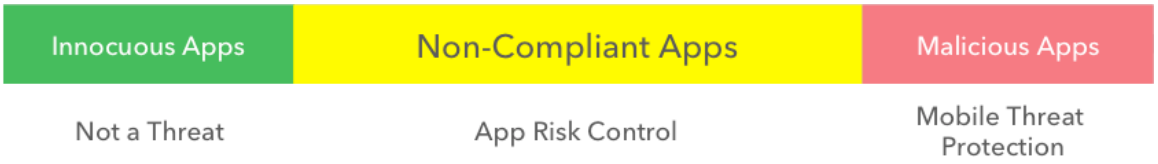
Mobility moves everything to the cloud and – by extension – the security solutions need to move too. According to Software Advice, in 2008, 12% of enterprises preferred cloud based solutions. Fast-forward to 2014, and 87% want cloud-based apps.



"More than 268 billion mobile app downloads will have taken place by 2017, generating more than $77 billion in revenue and "making apps one of the most popular computing tools for users across the globe," according to Gartner's "Predicts 2014: Apps, Personal Cloud and Data Analytics Will Drive New Consumer Interactions."

Security for mobility requires a different mindset, different tools, and new fundamentals. People want simultaneous access to work apps like Salesforce and personal apps like Facebook. Soon, they will expect mobile access to everything, including HR and line of business apps that likely hold highly sensitive information.

The sheer volume of available applications will require advanced, mobility focused, security tools to provide visibility into an application's capabilities and intentions. Many applications are not malicious, but may contravene the security policy of an organization or even violate regulatory requirements. For these non-compliant apps, admins need tools to both view and set actionable policies against apps that may be considered "risky".



Ultimately, the biggest challenge is to allow your business to be mobile and secure. Enterprise Infrastructures have to strike the right balance between securing technologies while enabling a highly productive workforce. Security solutions need to eliminate distraction from using mobile devices safely and effectively, allow for flexibility, and reduce data breaches. IT departments shouldn't have to forgo productivity for security, or limit security for mobility.

Gartner recently published its "Market Guide for Mobile Threat Defense Solutions" to establish a clear definition for Mobile Threat Defense (MTD).

Here is Gartner's market definition for Mobile Threat Defense:

"The MTD solutions market is made up of products that protect organizations from threats on mobile platforms, including iOS, Android and Windows 10 Mobile. MTD solutions provide security at one or more of these four levels:

1. Device behavioral anomalies — MTD tools provide behavioral anomaly detection by tracking expected and acceptable use patterns.
2. Vulnerability assessments — MTD tools inspect devices for configuration weaknesses that will lead to malware execution.
3. Network security — MTD tools monitor network traffic and disable suspicious connections to and from mobile devices.
4. App scans — MTD tools identify "leaky" apps (meaning apps that can put enterprise data at risk) and malicious apps, through reputation scanning and code analysis."

This definition is important because it makes clear what mobile threat defense solutions should protect against in enterprise environments and also further clarifies the role of MTD in securing mobility.

Mobile Operating systems have been designed to be more secure. Multiple security mechanisms have been implemented, such as developer programs; store scanning so any application is reviewed before being made available. On the device, sandboxing ensures that each app is executed in its own space and there are permissions required when apps need to access specific parts of the devices.... However, attackers have found ways to circumvent those mechanisms: Stolen enterprise certificates, evasion techniques to bypass review, jailbreak and rooting to unlock security as well as sideloading applications.

As mobile phones continue to be tightly integrated into our personal and work lives, malicious actors are actively creating sophisticated applications that can run on victims' devices without either their knowledge of the threat's presence, or of the actors' intent. This can be seen in the diversity of threats that target mobile devices: from those that are

financially motivated, such as adware, ransomware (banking) Trojans, and SMS fraud, to those seeking personal information or corporate intellectual property.

Attackers are going to follow the data and more of it is being stored on or accessed via mobile devices. Recently, Lookout discovered the some of the most advanced Spyware in use today.

https://www.lookout.com/trident-pegasus-enterprise-discovery

Spyware is a malicious application designed to retrieve specific information from an infected device without the victim's knowledge. These types of applications often include the ability to extract a victim's SMS messages, contact details, record their calls, access their call logs, or remotely activate a device's microphone and camera to surreptitiously capture audio, video, and image content.

Mobile threats are no longer the domain of individual users looking to make easy money off of simple attacks. It is becoming a more professional environment. Two private security firms, Gamma Group and Hacking Team, both made headlines after media outlets revealed that the organizations developed mobile surveillance software that has been sold to oppressive governments.

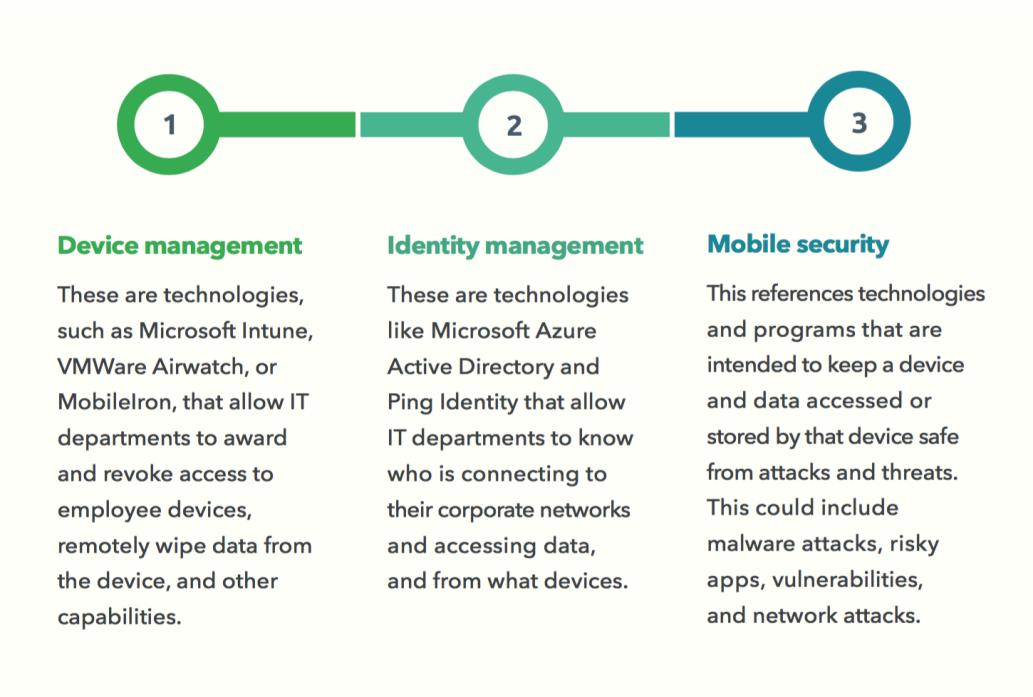
The Israeli based NSO Group has managed to avoid the spotlight of the cyber security community despite being in operation for over five years. Founded in 2010 by Niv Carmi, Shalev Hulio, and Omri Lavie, NSO Group has publicly stated that it develops and sells mobile phone surveillance software to governments and organizations around the world.

One of the most significant challenges that many IT organizations face is how to define a Mobile Policy that enables the benefits of a mobile environment, but does not sacrifice data and resource availability, integrity or confidentiality. Each organization needs to develop a

policy that outlines how its users will interact with their mobile environment. Typical concerns are, but not limited too:

1. Will mobile devices be corporate provided, BYOD or COPE?
2. Will only specific mobile operating systems be allowed?
3. How do I manage the security and management of the assets?
4. What are the acceptable risks?
5. What are the restrictions for installing applications?
6. How will devices be authenticated for access and what resources will be accessible?
7. What type of data can be stored on the device and how is that secured?
8. Can existing IT tools be leveraged to reduce costs?

Securing mobility is the umbrella for making sure that company- and employee-data remain safe while being used on mobile devices. There are three elements to securing mobility that every organization needs to consider.



When considering the challenge to address mobile security, several steps can be taken immediately:

1. Defining policies and best practices for the mobile environment is strong first step. Almost all employees these days have a mobile device that accesses some degree of company resources and data. Mobility technologies continue to trend to more enablement and access so it is important to get a clearly defined policy in place

early. Mobility by definition is a fast moving technology so mobile policies will need to be monitored and refined regularly.

2. Implement a holistic plan for securing mobile devices that covers the three elements described above; Device Management, Identity Management and Mobile Security. Most mobile solutions today are implemented with a patchwork of tools and workarounds and in many cases try to use network based tools. The mobile environment is vastly different from traditional PC/network based systems and it requires security and management tools that are developed from the ground up to support mobile devices.

   Mobile Security solutions should focus on these capabilities:

   - Application Based Threats - Mobile Malware and Vulnerabilities
   - Compromised operating systems
   - Sideloaded Applications
   - Network-based “Man-in-the- middle” attacks
   - Non-compliant or “Risky” Applications
   - Integration with existing IT systems

3. Develop a comprehensive training program for mobile users. The threats that are relevant to a PC are still relevant in many cases to a mobile device. Mobile devices also have additional threat surfaces that are not applicable to PCs and users are unaware of the risks (e.g. text messages, rogue wi-fi, etc…). A comprehensive training plan that details the various threats and best practices for using mobile devices will be critical to minimize mobile threats.

SUMMARY

The overall usage of mobile devices to increase productivity has grown dramatically over the last few years. As more business critical services become mobility enabled, in conjunction with expanded cloud based offerings, IT departments need to focus on how to secure their mobile data when it is no longer confined within the organizational domain. By providing visibility into mobile malware, compromised operating systems, network attacks, and non-compliant "risky" apps, Mobile Security gives you a holistic view of the overall threat ecosystem in which your business operates. Mobile devices have already proven to be a driving force for greater productivity and business enablement. Many IT departments are struggling with how to further amplify those benefits while still providing a secure environment. It is imperative to begin the process now of developing Mobile Policies, deploying Mobile Security tools and providing mobility training to the workforce to take advantage of those benefits and keep mobile devices secured.