

A new approach to mobile security: protection on every side

by Nicolas Severino, Director Systems Engineer, Latin America, Symantec

The numbers of mobile devices is set to exceed those of PCs, and they are getting smarter. Therefore, they should be protected to the same level as the PC in a holistic approach. The risk to the enterprise is even higher due to ‘consumerisation’ - personal use mixed with business use. Unprotected data on lost or stolen devices could damage the enterprise business and its reputation, let alone to individuals who use it for financial transactions. Protecting these mobile devices should cover all functions, for example, preventing mobile spyware that could operate the handset camera or microphone without the owner’s knowledge. Applying remote management and configuration enhances device security, and remote data wipe-out when devices are lost or stolen avoids breaching confidentiality of sensitive data.



Nicolas Severino is the Director of Engineering for Symantec in Latin America where he leads a team responsible for presenting protection solutions and information management to consumers and businesses in different markets. He and his team raise the appreciation of Symantec’s technologies, how they protect data and how they assist in achieving business goals. Nicolas has over fifteen years of experience in information technology in various companies, specializing in issues of information security, infrastructure and networking. He joined Symantec in 2001, where he held various positions related to Sales, Marketing and Engineering.

Every technological advance brings an increase in productivity, but it also includes an increase in risk. In the case of mobile devices, the advances introduced on a continuous basis are increasingly facilitating consumers to merge their personal and business lives. More digital devices are connecting to the Internet every day - devices beyond traditional PCs. In fact, according to IDC analysis, this year it is predicted that one billion phones will connect to the Internet globally, compared to 1.3 billion PCs.

Today’s smartphones and other mobile devices - along with the service provider networks they operate on - are highly sophisticated, and tomorrow will be even more so. Increasingly, these devices and subsequently the related service provider networks are being brought into the Enterprise by end-users.

This ‘consumerisation’ of IT offers tremendous productivity increases, but also creates new security and management challenges for IT

organizations, consumers and communication service providers, not only in Latin America, but also around the world. Given that modern mobile devices carry enormous volumes of data and connect across devices and networks using a wide array of connectivity standards, and that they are also used for financial transactions, the loss or theft of a device can result in direct revenue loss, legal ramifications and brand damage. Therefore, these challenges should not be ignored any longer.

To overcome these challenges, the mobile industry as a whole must begin shifting towards a holistic approach to mobile security and management in order to keep sensitive enterprise data secure. This complete approach should focus on shoring up the security of both the visible and the not-so-visible (from the enterprise perspective) mobile ecosystems. The not-so-visible ecosystem consists of the endpoints where the data is created, used and stored, and the network servers, through which the devices communicate with corporate backend servers.

Security for mobiles in Latin America

Protecting the mobile ecosystem: devices and data

As mobile devices become more sophisticated, provide greater corporate access and store more data, they become an increasingly popular target for attackers. Cyber-crime is a business. Moreover, as with a legitimate business, cyber-crime is driven by a return on investment. Symantec believes that this explains the current state of cyber-crime on mobile threats. All of the requirements for an active threat landscape existed in 2010. The installed base of smartphones and other mobile devices had grown to an attractive size. The devices are running sophisticated operating systems that come with the inevitable vulnerabilities - 163 counted in 2010 versus 115 in 2009, which represents an increase of 42 per cent.

Mobile devices also become a bigger target for theft, and their size makes them

much easier to misplace and get lost. Their computing power also makes them a convenient alternative to the traditional laptop. As a result, companies need to manage these devices and make sure that they are secure. They must avoid making exceptions for mobile devices and should treat them as they would any other endpoint.

By implementing solutions focused on protecting mobile devices - much like those used to secure data on PCs - organizations can ensure that mobile devices are not the weak link in their IT security armour. This includes mobile security, device management, information protection and authentication technologies:

- **Security:** Mobile threats are still in their infancy and are nowhere near at the level we see targeting traditional computing platforms. However, some creative cyber-criminals have found ways to exploit smart mobile devices through viruses, Trojans, SMS or email phishing, rogue applications and snoopware. Mobile snoopware is spyware that activates features on a device without the user's knowledge, such as the microphone or camera. It is increasingly important to employ mobile security solutions that provide a barrier against these attacks. Security solutions that feature network access control can also help to enforce compliance with security policies.

- **Device Management:** A well-managed device is a secure device. It is important that mobile devices remain properly configured and managed at all times, using mobile device management (MDM) solutions. By increasing IT efficiency with over-the-air deployment of configurations, applications and updates, these management solutions help to ensure that devices comply with the required policies, that they are configured correctly and kept up-to-date. This not only improves end-user productivity but also minimises vulnerabilities on the devices.

- **Information Protection:** The biggest threat to mobile devices remains the risk of loss or theft. As more companies use these devices simply as additional endpoints, data stored on them is put at even greater risk. Corporate email and data from line of business applications on smartphones often contains intellectual property or information subject to government confidentiality regulation. The loss or theft of the device exposes sensitive data and may result in financial loss, legal ramifications and brand damage. Strong password/PIN policies prevent unauthorized access to the mobile device and its data. Mobile encryption technologies provide protection for data communicated and stored on mobile devices. Remote wipe and lock capabilities enable

the enterprise to delete all of the corporate data on the device remotely to ensure that the data cannot be breached. Organizations need a granular control over these remote wipe capabilities so that only the corporate-owned data can be wiped out, not personal data. Finally, enterprises need to make sure that appropriate data leakage prevention policies are in place to reduce the flow of sensitive data out of the mobile devices.

- **Authentication:** Most enterprise networks require a username and password to identify users, but usernames and passwords can be compromised. Using two-factor authentication technology provides a higher level of security when users log in to the corporate network. Quality authentication technologies extend the same safety measures for when users log in from a mobile device. As enterprises develop custom applications, they need to look at extending the authentication to these apps as well.

Protecting the not-so-visible ecosystem: service provider networks

As more and more enterprise endpoints access the service provider networks directly (via mobile devices), organizations need to feel comfortable that the vital service provider networks their mobile devices connect to are also free of attacks and threats that could proliferate into their own systems. Superior mobile security and comprehensive network protection allows the service providers to provide that confidence to enterprises.

- **Network Protection:** As malicious threats designed to be propagated via mobile networks increase, so too must the measures implemented by providers to block these threats. Service provider networks should be protected at their edge, never allowing these threats to get in. By building a network-wide policy control and enforcement system, these networks are guarded against malware. A network-wide solution must include an application-level security policy that protects the predominant types of traffic entering the network, including web browsing, SMS, MMS and so on.

- **Services Revenue:** Improving overall security with a network-wide policy control and enforcement solution has additional benefits. It empowers providers to offer revenue-generating protection services for both enterprises and consumers. These include enterprise-level control of permitted web browsing and control of what devices connect to the enterprise infrastructure. These capabilities can be sold as a Security-as-a-Service (SAAS) to enterprises to attract and retain corporate customers. They can also be offered as consumer level control capabilities,

providing individual subscribers control over their mobile presence across all services.

- **Security Insight:** In order to protect network stability, performance and subscriber trust, it is critical that service providers have real-time insight into what types of activity are happening within their network. Real-time control is often required in order to comply with increasing regulatory requirements being placed on them. An intelligent security solution designed to identify, manage and report suspicious activity in real-time, enables a proactive approach which improves network efficiency by allowing only valid traffic to traverse the network. Operators must ensure they store and retrieve application data requested by enterprises, helping meet regulatory requirements for data retention and recovery.

Some consumers and organizations do already recognize the challenges and potential pitfalls that come with the world of connected smart devices. Respondents to a 2010 Mobile & Smart Device Security Survey acknowledge that device security problems are not only inevitable, but also potentially serious. (source: Mocana)

- 71 per cent of respondents expect a serious incident arising from attacks or problems with connected smart devices within the next 24 months.
- 65 per cent report that attacks against their smart devices already require the regular attention of their IT staff, or will start requiring it this year.

However, with the consumerisation of IT, many employees want to use the devices they prefer and are less willing than ever before to live with corporate IT mandated devices. Choice is the new paradigm. Employees wish to use a single device that fits in their pocket, and has the computing power of today's laptops, so they can take their computer with them and access their data no matter where they are. They do not realise that in the event of the device getting lost or stolen, they may be putting their company at risk financially, and jeopardizing its security.

As we continue to plunge into this new era of mobile computing where smart mobile devices are becoming more common than laptops and desktops, providing comprehensive security for the devices and the networks in which they communicate seems a daunting challenge. However, it is not an impossible task. The key is an industry-wide holistic approach that stops making exceptions for mobile devices and treats them as true endpoints. Ideally, this would include integrated protection solutions for end-users, enterprises and telecommunication service providers. ●