Mobile Security:

Controlling Growing Threats with Mobile Device Management

LabTech™

As the use of mobile devices continues to grow, so do mobile security threats. Most people use their mobile devices for both work and leisure, which creates even greater risks.

And since mobile devices are always on and carried from home, to work, then the coffee shop and everywhere else, opportunities for security breaches from malware and lost or stolen devices are multiplied. The threats and risks, ranging from unauthorized access to data stored on mobile devices to a device's ability to access corporate networks, can't be underestimated.

The Bring Your Own Device (BYOD) model is particularly attractive to employees because it provides greater mobility, improves efficiency and productivity, and increases job satisfaction. At the same time, BYOD further complicates data security for IT departments.

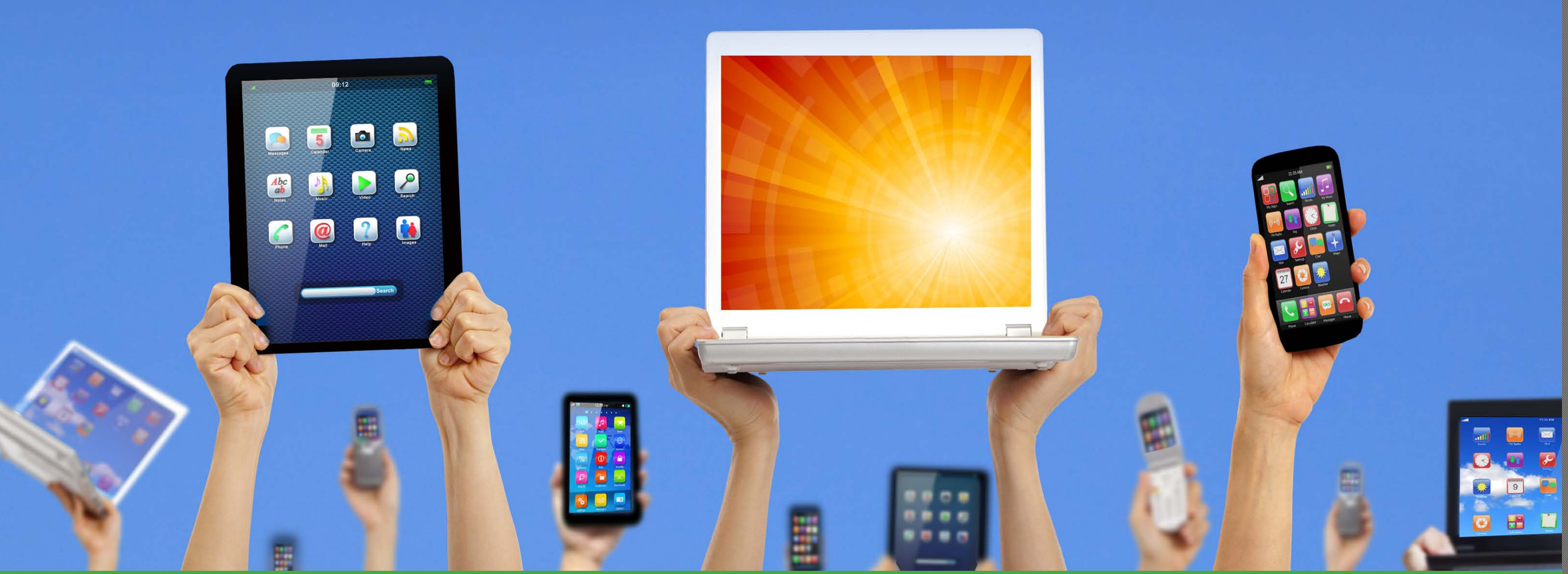
Seventy percent of IT professionals say the security of mobile devices is the largest risk to deal with when building a mobility strategy, according to a survey by CompTIA. A lost or stolen device is the most common type of mobile security incident, with 56 percent surveyed reporting this experience. Other concerns include unauthorized applications, malware and the protection of data. Even though many IT professionals require employees to use passcodes and encryption to protect the data on mobile devices, those same IT professionals feel more advanced security techniques are necessary.[1]

1 Mobile Device Management: Protecting Multiple Mobile Devices

As increasing numbers of employees use mobile devices, there's a greater need for IT managers to support them. Smart IT services providers are casting their safety net wider by introducing mobile device management (MDM) systems. Mobile device management includes a range of products and services that let IT managers prevent malware and manage other risks, such as lost or misplaced devices and improper employee behavior.

With the right MDM solution, IT service providers can help IT departments tie their mobile devices to their legacy systems while providing key security measures.

Although many IT departments are implementing mobile device policies to prevent security issues, those policies are often not enough and can be tough to enforce. MDM takes security a step further by becoming an important monitoring and enforcement tool. By offering MDM, IT service providers can also lighten the burden on overtaxed IT departments while generating additional revenue.

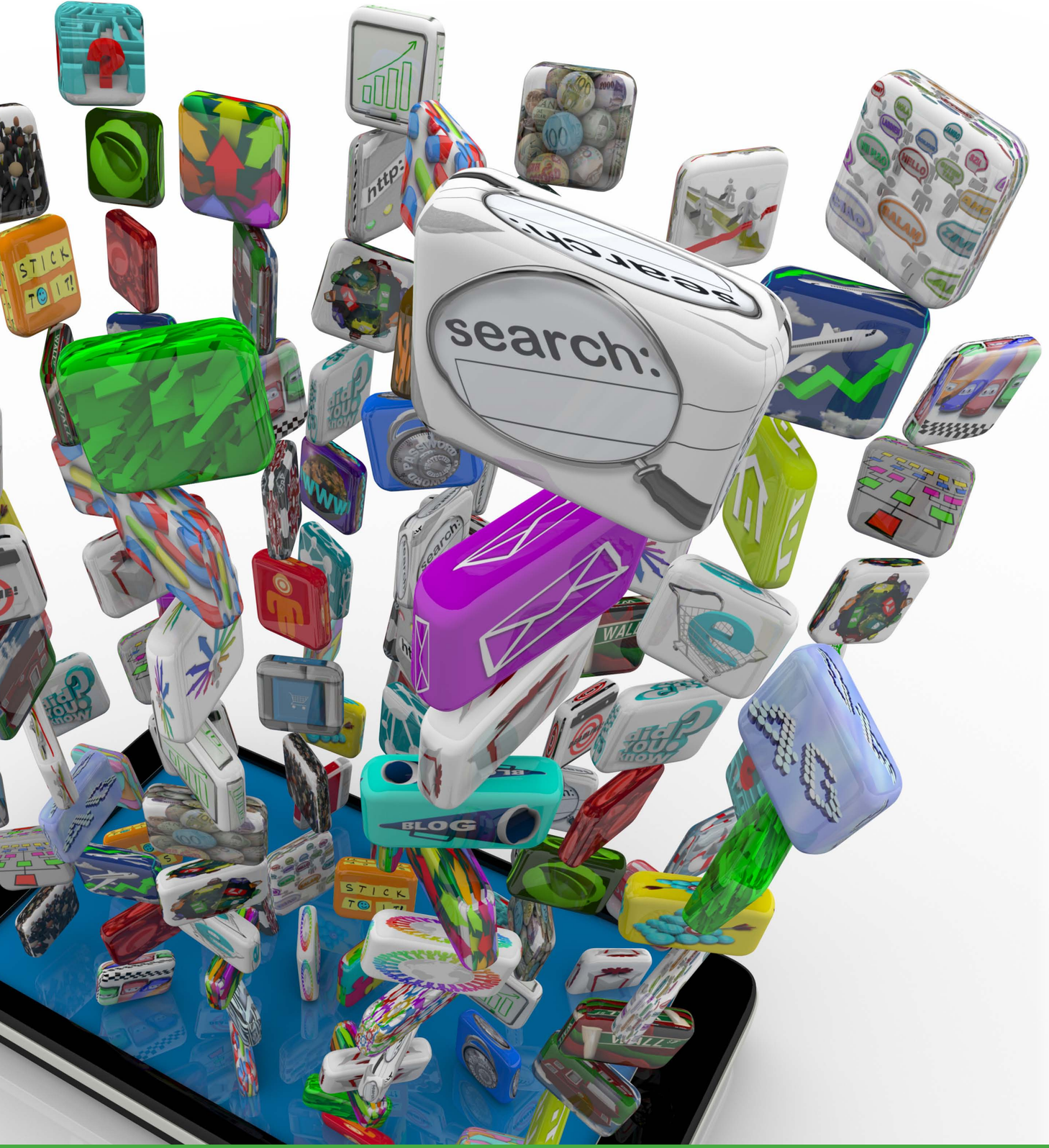


What to Look for in an MDM Tool

When reviewing an MDM tool, look for one that integrates with your professional automation software (PSA) to provide maximum efficiency and productivity. An MDM tool should also offer a comprehensive list of options, such as the ability to:

- Safely enroll new or existing devices over-the-air (OTA).
- Configure one or multiple devices to enforce company policies and procedures.
- Collect and analyze relevant hardware and software data, such as device type, model, serial number, memory and installed apps.
- Collect hardware data, including processor, memory, hard drive space and battery life. Also, view and manage inventory of installed applications.
- Capture carrier network, phone number and data roaming settings.
- Secure customers' networks through safety policies and restrictions.
- Enforce restrictions, such as access to the app stores, camera and browser security.
- Define password complexity for unlocking the phone and number of failed login attempts before all data on the device is erased.
- Centrally manage all mobile devices across all customer sites from a single interface.
- Remotely reset passcodes, lock devices and wipe devices.
- Safely apply corporate settings, including Microsoft Exchange, Wi-Fi, VPN, LDAP, and configure and apply third party email such as POP and IMAP.

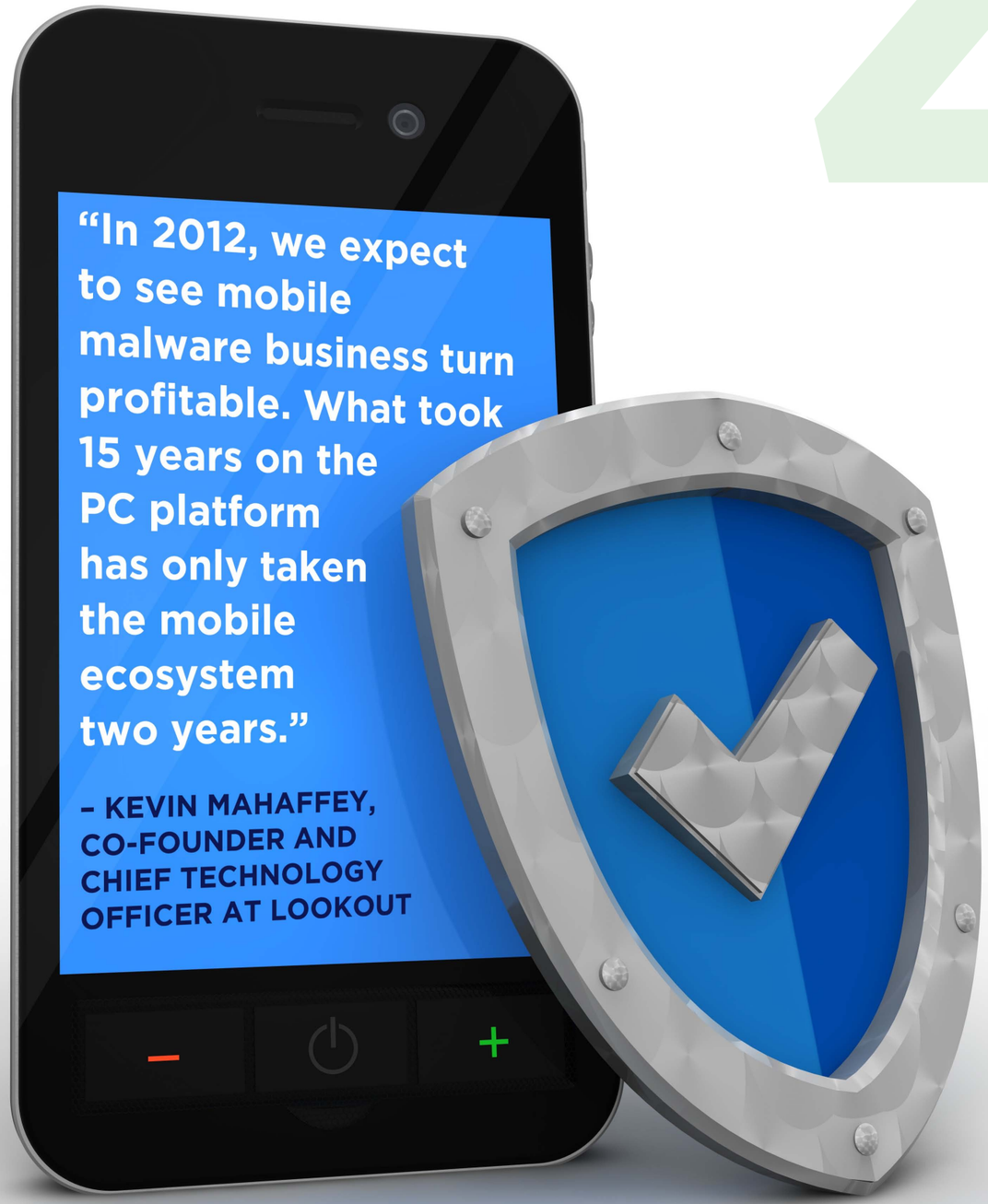
LabTech Software, the developer of a powerful remote monitoring and management (RMM) platform, recently introduced MDM to serve the growing mobile market. LabTech MDM is a powerful, fast and easy-to-use tool that allows IT service providers to manage and secure Android™ and Apple iOS® mobile devices remotely, safely and efficiently throughout their entire lifecycle.



3 Mobile Use is Growing

With the rapid growth in mobile devices, it's easy to see why mobile security has become a top priority. Nearly 4 billion mobile phones were used worldwide in 2011, and nearly 1.08 billion of those were smartphones. That rate is growing so fast that by 2014, mobile Internet should take over desktop Internet usage.[2]

Mobile devices aren't just limited to smartphones. They also include iPads and other tablets, and their popularity is growing as well. Tablet sales are forecasted to reach nearly 500 million units by 2015, compared to 95 million sold in 2011.[3] Those mobile devices will enter the business market at a rapid pace.



4 Malware Threats Growing Rapidly

If the proliferation of mobile malware in 2011 is any indication, there is good reason for concern. Hackers are always looking for new targets because IT departments are getting much better at securing their networks. Mobile devices have become that new, easy target.

While 2011 was considered a bad year for malware, 2012 is expected to be even worse, especially for users of Google Android, the leading mobile platform. The likelihood of an Android user encountering malware at the end of 2011 had increased to 4 percent, up from a 1 percent likelihood at the beginning of 2011, according to Lookout's 2012 Mobile Malware Predictions.

"In 2012, we expect to see mobile malware business turn profitable. What took 15 years on the PC platform has only taken the mobile ecosystem two years," says Kevin Mahaffey, co-founder and chief technology officer at Lookout.[4]

There was a 155 percent increase in mobile malware across all platforms in 2011 and a 3,325 increase in Android malware in the last seven months of 2011. The most dominant type of mobile malware affecting Android was spyware (63 percent), which can capture and transfer data. SMS trojans account for 36 percent of mobile malware, which can send SMS messages to premium rate numbers owned by the attacker. Just as disconcerting, a large number of applications are considered suspicious, collecting information or asking for permissions that are over-reaching, dubious or unethical. They pose a threat to privacy because they share unnecessary information with third parties.[5]

Even more troubling is the source of malware. An analysis by ESET Latin America showed that 30 percent of malware threats were downloaded from the official manufacturer's repository. Most threats (70 percent) were downloaded from non-official repositories.[6]

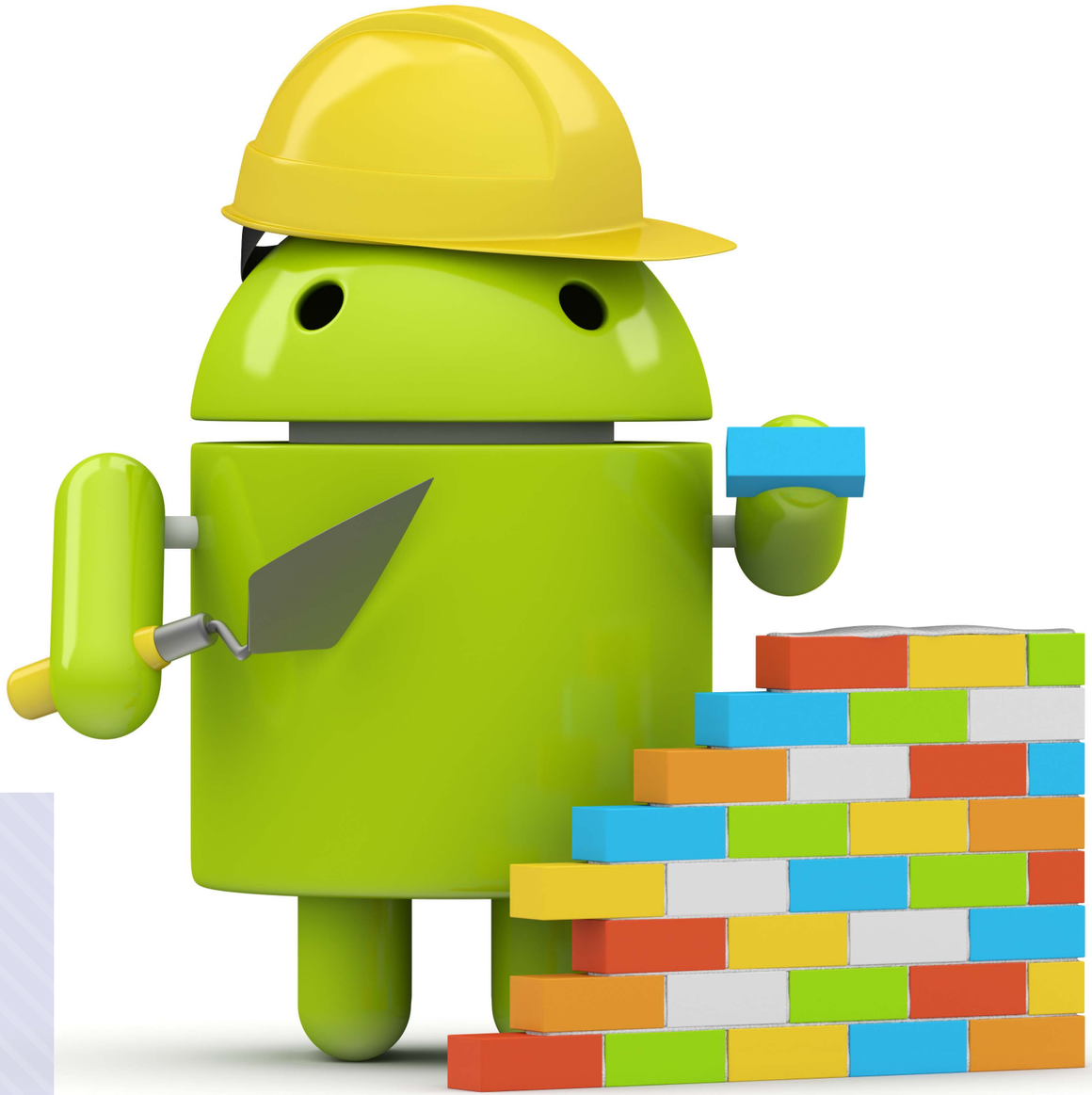
5

Not Just Android

Even though the focus is on Android, all mobile operating systems are susceptible, including Apple iOS, Symbian, Windows® Mobile and Blackberry®.

Although Apple iOS phones have the reputation of being malware free, this is a common misnomer. Apple's review process prevents suspect software from being sold in Apple's App store, but malware can infect jailbroken iPhones, which allows users to run software not authorized by Apple.

So, even though devices that run Apple iOS have a solid reputation for security, iPads and iPhones must also be part of an MDM strategy.



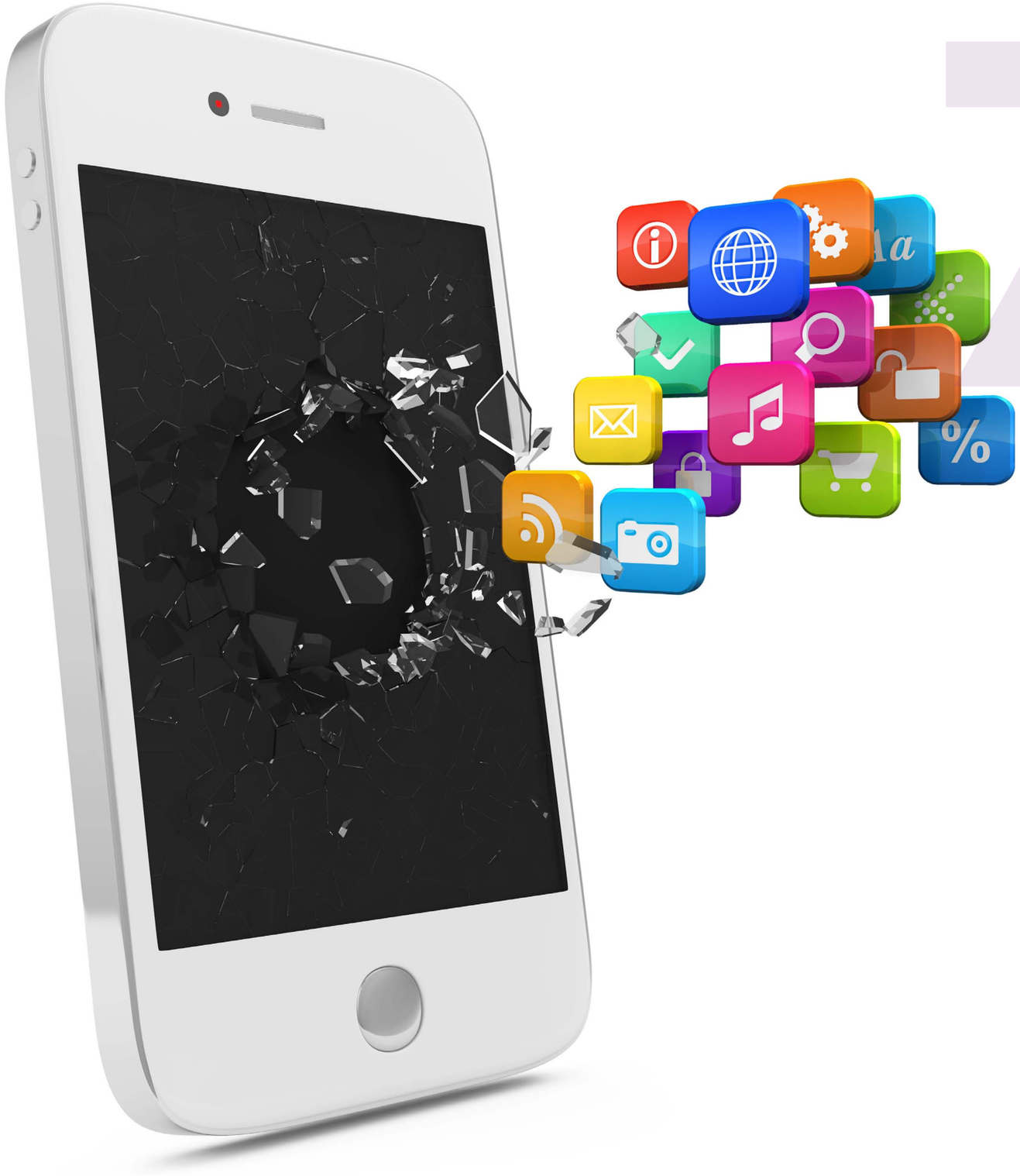
"There was a 155% increase in mobile malware across all platforms in 2011, and a 3,325 increase in Android malware in the first seven months of 2011."

– JUNIPER NETWORKS

6 Your Data Sold for Profit

When malware first appeared, it seemed to be driven by mischief or bragging rights. As mobile platforms mature and the potential for rewards increases, the authors of malware will become more profit driven.

Since users often use their mobile devices for storing and accessing banking information and company information, the risk of losing sensitive data is increasing. In 2008, bank account credentials were worth $10 to $1,000 and email passwords were worth $4 to $30 on the black market.[7] The value of company-related data could be far greater.



Study Highlights Dangers of Lost Phones

While many mobile device users may be extra careful about keeping mobile malware off their portable device, some things are unavoidable, such as loss or theft. What's really scary is what could happen when someone else finds those phones. Symantec planted 50 "lost" phones in five cities across the United States and Canada, then remotely tracked them to determine what data was accessed when they were found.

Security software or passwords were not enabled on the devices. Of the lost phones, 83 percent of the devices showed attempts to access corporate-related apps or data.

Attempts to access a corporate email client occurred on nearly half the devices, and a file titled "HR Salaries" was accessed on 53 percent of the phones. Only half the finders contacted the owners and provided contact information.[8]

Based on the studies above, chances are pretty good that a cell phone user will lose his or her phone, and chances are even greater that information on a found phone will be accessed if proper security software or features aren't in place.

Summary

As the popularity of mobile devices grows, the opportunities for security breaches grow as well, placing a new burden on IT departments. By offering mobile device management services, IT service providers can ease that burden while expanding their managed services offerings. When choosing the right mobility solution, look for ease of use, flexibility and a wide range of management options.

A comprehensive MDM solution helps provide effective risk management, minimizes security threats, ensures policy compliance and regulates employee behavior, all without getting in the way of the features that make mobile devices such an integral part of business. An MDM solution allows users to continue using their devices to increase productivity and efficiency, without worrying about security threats.

About LabTech Software

LabTech is the only managed services tool for remote monitoring, management and automation developed by a managed service provider (MSP) for MSPs. Their affordable, agent-based solution so closely emulates what technicians do in the field that the techs can provide the same support remotely. Because LabTech Software understands how to manage a growing MSP business, they make it easier to procure their software and allow partners to add agents as they grow. For more information, please visit labtechsoftware.com

LabTech™

4110 George Road, Suite 200 | Tampa, Florida 33634
877.522.8323 | labtechsoftware.com

1 "Fast Facts on the Mobility Market," CompTIA, 2011.

2 Richmond, Holly, "The Growth of Mobile Marketing and Tagging," March 21, 2011, http://tag.microsoft.com/community/blog/t/the_growth_of_mobile_marketing_and_tagging.aspx.

3 Cocotas, Alex, "Tablet Market Forecast: Sales Will Reach Nearly 500 Million Units by 2015," Business Insider, Feb. 14, 2012, http://articles.businessinsider.com/2012-02-14/research/31057816_1_tablets-smartphones-pc-sales.

4 Rao, Leena, Lookout's 2012 Mobile Security Threat Predictions: SMS Fraud, Botnets and Malvertising, Dec. 13, 2011, http://techcrunch.com/2011/12/13/lookouts-2012-mobile-security-threat-predictions-sms-fraud-botnets-and-malvertising/.

5 "2011 Mobile Threats Report," February 2012, Juniper Networks.

6 "Trends for 2012, Malware Goes Mobile," ESET Latin America, January 2012.

7 "Symantec Report on the Underground Economy, July 07-June 08," Symantec Enterprise Security, November 2008.

8 "The Symantec Smartphone Honey Stick Project," Symantec, 2012.