White Paper

Nine Critical Threats Against Mobile Workers

Criminals, hacktivists and hostile governments understand that the quickest way to corporate data is through mobile workers' unsecured endpoints.

MARBLE

Table of Contents

Introduction

Cyber criminals targeted mobile devices at unprecedented rates in 2012, exploiting the weakest link in the corporate network to steal enterprise information. For the first time, malware attacks on mobile devices exceeded attacks on PCs in the U.S. and Australia.[1] Attacks to smart phones, tablets and laptops will only increase in the years ahead, industry experts say.

Converging on IT and security professionals are several broader trends within the enterprise that expose networks, applications and devices to attacks. Consider that:

- 66 percent of information workers in Europe and the United States work remotely beyond the firewall[2]
- An increasing amount of corporate data now resides in external and internal clouds
- Corporate data is accessed from non-secure and non-corporate controlled networks, such as Wi-Fi hotspots

The net result is that hackers, hacktivists and hostile governments understand that the quickest way to the corporate data they seek is through mobile workers' unsecured endpoints.

How big a priority is securing mobile devices for IT? According to Gartner, only 27 percent of CIOs queried for a recent study believed that their mobile security would satisfy an auditor.[3] Call it the downside of the bring-your-own-technology paradigm shift. While BYOT policies save IT countless dollars purchasing, provisioning and maintaining mobile devices, IT's job going forward must be managing and controlling risk.

The challenges of limiting risk around employee-owned mobile devices are real and complex. Mobile device management (MDM) solutions have proved effective in a limited way, particularly enforcing device policies, password control, VPN, and remote wiping capabilities for lost or stolen smart phones and tablets. MDM solutions, however, do not protect against the continuous security attacks facing companies and government agencies.

To sufficiently reduce risk IT must deploy separate solutions for controlling access to their networks, security intelligence, analytics and reporting – capabilities that far exceed current MDM solutions. Faced with dwindling budgets and technically sophisticated criminal organizations focused on stealing information or shutting

[1] "Sophos Security Threat Report 2013: New Platforms and Changing Threats," 2012 p. 14.

[2] "Demystifying The Mobile Workforce," TJ Keitt, Forrester, June 7, 2011, p. 2.

[3] "CIO Attitudes Toward Consumerization of Mobile Devices and Applications," Nick Jones, Gartner, May 2011, p. 6.

down government agencies and enterprises, CIOs must make difficult choices about what they can and cannot protect.

What's needed is a mobile security management solution that protects the enterprise against the ever-changing threats introduced into enterprises by mobile devices that simply cannot be mitigated by standard MDM solutions. Such a solution must secure remote workers' access to corporate networks and cloud services on Android and iOS mobile devices, as well as Windows and Mac computers.

This white paper seeks to describe nine schemes used by criminal entities targeting employee-owned mobile devices to penetrate the corporate firewall and the risks they pose. The threats discussed here include:

1. Malware, trojans and zero-day attacks
2. Key loggers
3. Compromised Wi-Fi hotspots
4. Poisoned DNS
5. Malicious and privacy leaking apps
6. Jail broken and rooted devices
7. Unpatched OS Versions
8. Spear phishing
9. Advanced persistent threats

In addition, this white paper will discuss the latest strategies to protect against these varied attacks and a road map for reducing the risk unleashed by compromised mobile devices.

1. Malware, Trojans and Zero-Day Attacks

Malware is generally seen as impacting PCs running the Windows operating system, however there is certainly an increasing amount of malware targeting users of Apple's Mac OS and mobile devices. Commercial antivirus software is about 80 percent effective in protecting against malware, crimeware, and zero-day attacks. Sometimes, depending on the commercial antivirus products used, that detection rate can be less than 25 percent.[4] While these solutions are an important defense, they will not completely protect enterprise users from virus infection because malware authors are creating new samples at unprecedented rates.

[4] "A Closer Look: Email-Based Malware Attacks," Brian Krebs, krebsonsecurity.com, June, 12, 2012.

In 2012 alone there were approximately 34 million new pieces of unique malware distributed, bringing the total amount to a whopping 90 million pieces, according to The AV-Test Institute, one of the leading providers of IT security and anti-virus research.[5] These figures include polymorphic malware, which generates a unique sample for each user.

But the most significant new targets for malware are mobile devices, as criminals increasingly attack employee-owned smart phones and tablets to penetrate the corporate firewall and scan enterprise networks. According to McAfee's most recent threats report, mobile malware saw a 700% increase over 2011, with more than 13,000 unique mobile malware samples identified in 2012 alone.[6] Android is clearly the number one targeted platform, with Symbian a distant second.

Anti-malware software scanning solutions for mobile devices are not nearly as sophisticated as those for PCs. As a result, it's terrifying to realize the potential ramifications of an employee using an infected Android tablet or a Galaxy phone to access corporate infrastructure, such email, cloud services, or the internal network.

Drive-by malware attacks on mobile devices have become prevalent on Android devices. With the drive-by strategy, criminals redirect visitors of a website to one they control, whereupon the malware automatically installs itself on the user's Android device, basically rooting it. Once the malware takes over the device it may track data from applications, monitor network traffic, GPS information and even the user's keystrokes, ultimately sending all this information to third party servers.

A Solution to Malware, Trojans and Zero-Day Attacks

Continuing the arms race against the exploding malware problem has proved to be a zero-sum game. The best approach for IT is to completely isolate users from unknown malware by creating a virtualized security environment, particularly on Windows and Mac computers. This approach uses a virtual machine that runs an NSA-hardened Linux environment that is separate from the computer's Windows or Mac operating systems. From this highly secure environment, which can include watchdog processes, a user can run VPN services and browsing. This approach effectively isolates the user against new malware and zero-day attacks on the most popular operating systems.

Similarly, Android and iOS devices can also take advantage of isolating and sandboxing technologies to create virtualized browsing environments that restrict access to websites set-up to infect mobile devices with malicious content.

[5] AV-TEST GmbH, "Statistics for Malware," www.av-test.org, 2013.

[6] "McAfee Threats Report: Second Quarter 2012," pp. 4-5, 2012.

2. Key Loggers

Key loggers, or keystroke logging, is a decidedly old-school hack, but still remains one of the primary ways cyber criminals compromise virtual private networks, corporate networks, email accounts and online banking sites. Basically, the hacker inserts a driver beneath the operating system and tracks everything the user types, sending the information to third party servers where sign-on credentials can be exploited.

While key loggers have become more sophisticated, they've also gone cross platform. We used to only worry about them on the Windows platform, but they've also become available on the Mac platform, primarily through malicious apps that users are tricked into downloading.

Increasingly, key loggers have targeted both Android and iOS devices. One strategy is to jailbreak or root the device and install a key logger directly on the device. Another way is for hackers is to publish a tampered-with virtualized keyboard for iOS or Android – such as the Emoji Keyboard, which lets users insert small icons within text or email messages – so that every keystroke on your iPhone, iPad or Android device is recorded and sent to a third party server.

A Solution to Key Loggers

An approach to solving key logging on the Windows and Mac platforms is installing a driver beneath the operating system that encrypts all keystrokes to the application within a secured virtualized operating system. This method will potentially stop key logging before it can take over the device. If key strokes are sent to third party serviers, hackers will only see an encrypted stream of communications and will be unable to steal users' credentials for VPN or online cloud services.

For Android and iOS devices, scans should be conducted that discover known malicious apps and suspicious behavior, such as sending data from the device, and access to the network denied until the apps are removed.

3. Compromised Wi-Fi Hotspots

With Wi-Fi hotspots virtually everywhere, information workers are connecting to the Internet to access corporate services from coffee shops, airports, airplanes and hotels. In most cases public Wi-Fi hotspots may lack firewall protection, web filtering, or web intrusion systems. In every case corporate data is vulnerable whenever an employee logs into a Wi-Fi hot spot.

Wi-Fi networks are frequently configured so users can see everyone who's on the network. For instance, if an employee uses a non-encrypted connection to access

Facebook, email or SharePoint, their session can be easily hijacked by a hacker on the network. How easy is this to do? FireSheep, a commercial, downloadable app, allows users to see any non-encrypted connection on a network and hijack sessions. Once a hacker gets into an employee's Facebook account, they can send emails to friends, malicious links, and malware. In addition, the hacker also knows a great deal about the employee: their name, what they look like, possibly where they're traveling. Essentially, any kind of traffic can be intercepted over most hotspots.

More important, users typically can't assess what entity is providing the Domain Name System (DNS) from a hotspot. DNS services allow users to type a domain name in their browser and directs them to the IP address of a destination website. Hackers regularly scan Wi-Fi networks, log into them, and redirect traffic to a malicious DNS server, where they can point an employee to a bogus site that looks like your company's. When the unsuspecting employee logs into the pirate site, they surrender their password and credentials, and the hacker gains access to your corporate network.

In addition, criminals can be man-in-the-middling all Wi-Fi traffic and spoof any website. An employee user may think they're logging into their Gmail account, or your corporate site, but they've been tricked and the hackers have captured login information that can be exploited.

A Solution to Compromised Wi-Fi Hotspots

Employees must have a way to encrypt all communications over Wi-Fi hotspots from end-to-end. Enterprise VPN must be pre-configured to ensure that it's running before connecting to any enterprise service. If a company does not have VPN and remote employees are connecting to salesforce.com or some other cloud service, the connection should run through a private, third party VPN to prevent session hijacking and man-in-the-middle schemes. With this approach, hackers running compromised DNS or ISPs cannot snoop on the traffic and target users' destinations. Similarly, applications on Android devices, iPhones and iPads can be protected in the same way to assure that they go to the servers they're designed to visit.

4. Poisoned DNS

Typically, DNS is not viewed as a danger to enterprise security, but it is a mistake, particularly for mobile wokers. Most devices, regardless of platform, are preconfigured to use the DNS served up by Wi-Fi hotspots, ISPs, telecoms, or even the hotel where your employee is using the house internet service. Essentially, we're being asked to trust the DNS server provided to us, yet it's impossible to know anything about that DNS server.

In late 2012 there were two attacks in Romania and Pakistan, where DNS servers were poisoned and entire countries were routing traffic to fake, malicious websites. So this means that a user can type www.mybank.com and the DNS will point them to a different server that takes them to a website that looks like their bank, when it is actually a transparent proxy designed to steal passwords. This scheme can also be used to target a VPN endpoint to trick users into disclosing VPN passwords.

A Solution to Poisoned DNS

What's needed to protect against poisoned DNS is a separate, private and secure DNS service that can be accessed by employees' mobile devices -- whether running Windows, Mac OS, Android, or iOS. Users must be able to access this secure DNS service through a third party VPN service that ensures they are directed to valid Web sites. This practice will override connecting to the DNS served by the local Wi-Fi hot spot, ISPs, hotels or airports.

In addition, the secure DNS service can be further strengthened by integrating it with a real-time blacklist service that will prevent employees from visiting web sites that are known to either distribute malware or phishing webpage.

5. Malicious and Privacy Leaking Apps

Not every app that we have on our smart phones or tablets are secure. If we're only using the Apple App Store or Google Play to obtain applications for our iOS and Android devices, and we're not using a jail-broken iPhone or rooted Android device, there should be a relative sense of security.

However, there are still dangerous applications that can leak sensitive corporate information from those devices. For instance, an employee may install a game or a productivity app that asks for access to their address book, which may contain the names and critical information of every employee in your organization since employee address books are connected to Microsoft's Active Directory. The app will then send the entire contents of the address book to a server on the Internet, which could be stolen by hackers. That means there might very well be a database in the cloud that contains all the names, titles, phone numbers, and email addresses of each of your employees. With access to this information, hackers have everything they need for spear phishing and advanced persistent threats.

In yet another scheme, malware writers are downloading real applications from the Google Play marketplace– such as Angry Birds, Instagram, or the Opera web browser for Android –and inserting malicious code designed to steal information. Once the malicious app has been reconfigured for their purposes, hackers post them on third party marketplaces where they are downloaded at will by anyone. With more than

120 third party Android marketplaces available, it's unreasonable to expect employees to install applications only downloaded from Google Play.

Malware writers have also begun creating malicious online banking apps. The original apps are downloaded from legitimate sources, then modified to be one-time password tokens for online banking. Emails are then sent to the bank's customers to invite them to download the malicious apps. When used by unsuspecting bank customers, the fake tokens allow criminals to take over the user's bank account.

A Solution to Malicious and Privacy Leaking Apps

What's needed is a cloud service that scans all the apps on a mobile device and integrates with a real-time service that rates both malicious apps and apps that leak privacy information. IT can then establish policies that forbid access to the network by any device with an installed malicious or privacy leaking app, and guides the employee through the process of removing it from their device.

6. Jail Broken and Rooted Devices

Jail-broken iPhones and rooted Android devices are by definition completely unsecured and should always be prevented from accessing corporate networks. Sometimes an employee may not even know that their iOS or Android device has been jail broken. Perhaps the employee's teenage child has decided to jail break their parent's iPad to download an app for free, and the employee has no idea the next time they log into corporate services that they are using a compromised device.

A Solution to Jail Broken and Rooted Devices

Algorithms that detect jail broken and rooted devices can be used in conjunction with policies that prohibit network access to these severely compromised devices.

That said, detecting rooted Android devices is still quite difficult because there are so many variants of rooting software. In some cases, root kits have been designed to hide themselves within the operating system. In short, it's getting more and more difficult detecting whether a user's Android device has been commandeered.

7. Un-patched OS Versions

Allowing employees access to the corporate network with unpatched versions of operating systems is clearly one of the greatest security threats. Older versions of operating systems are almost always vulnerable to zero-day threats, known threat factors, and malware designed to attack specific versions of the operating system.

A Solution to Un-patched OS Versions

It's now possible to record the version of the operating system for Android and iOs devices and post it when the employee logs into the network. Administrators can then set policies whether to allow access to the network to the employee using a device with an unpatched OS.

The best approach for protecting Windows and Mac OS computers with unpatched operating systems is by using a virtualized security environment. By using a virtual machine running an NSA-hardened Linux environment, the unpatched OS is completely isolated from the network, allowing the employee to run VPN services and browse securely. This approach would effectively allow an employee logging into the network from their home PC with a very old Windows 98 OS, to access a virtual and highly-secure operating system that protects the corporate network.

8. Spear Phishing

Spear phishing – the practice of targeting specific users' information within a corporation, rather than every subscriber to eBay or PayPal, – is a significant threat to businesses and government agencies. Spam filters have been an effective defense against emails used by hackers, yet more than 300,000 new phising sites a month were discovered in 2012.[7]

There are two kinds of spear phishing attacks that have proven most effective: a general email attack targeting employees of a specific company and SMS phishing.

For the typical email attack, the hacker obtains an employee's email address and sends a message with a malicious link or file attachment. The employee may read the message while in a meeting and unwittingly hit the link in the email that takes them to a phishing site that installs malware. The employee may know better, but they're multi-tasking, looking at a small screen and probably not using their best judgment. Still the bad guys get the information they seek.

SMS phishing, or smishing, is the practice of texting people phishing emails that try to get users to log in to their banking or PayPal accounts, or more insidiously, their corporate network.

A Solution to Spear Phishing

Similar to the solution discussed in the "Poisoned DNS" section of this paper, what's needed to protect against spear phishing is a separate, private and secure DNS service that can be accessed by employees' mobile devices. Employees access this super secure

[8] "Safe Browsing – Protecting Web Users for 5 Years and Counting," Niels Provos, Google Online Security Blog, http://googleonlinesecurity.blogspot.com.au, Chart 1

DNS service through a third party VPN service that ensures they are only directed to valid websites and prevents visiting any spear phishing sites. Integrating the DNS server with a real-time white listing service that prevents employees from visiting sites that aren't approved by IT can further strengthen protection.

9. Advanced Persistent Threats

Advanced persistent threats, or APT, is a sophisticated name for attacks by criminal organizations that have the resources and the time to figure out a way to get into any corporation's network. These sophisticated and well-organized gangs may seek access to: ATM switches to change limits because they have a cache of stolen credit card accounts; ACH to move money; and account systems to move money between accounts. They may even figure out how to get into retail point-of-sale systems and man-in-the-middle those transactions, or remotely push firmware updates into those point-of-sale systems.

We've seen some of the most sophisticated and highly secured corporate networks fall to advanced persistent threats. For instance, RSA Security was breached in 2011 and its entire database of RSA tokens was stolen during a six-month attack. The way the cyber criminals targeted RSA was very simple: phony emails supposedly coming from the human resources department were sent to a half dozen employees advertising open job requisitions. When the employees downloaded the infected PDF file attached to the message, the bad guys got into the network.

Once malicious software is on an end user's device and connected to your network, either at the office or through VPN, the bad guys are free to break into your Active Directories, escalate privileges on different servers, and survey everything in your network.

A Solution to Advanced Persistent Threats

Needless to say, protecting your employees is the first line of defense against advanced persistent threats. The end user is most vulnerable to attacks on their own devices, on all platforms, either at home or when they are on the road. The best defense against these attacks is a layered solution that combines virtualization, tracking, network security and DNS security that in effect creates a secure, isolated environment that's always clean.

Minimizing Risk to Mobile Threats: Marble Security

Marble offers a mobile security management service that protects against the ever-changing threats unleashed into enterprises by mobile devices described in this paper. Simple to use and deploy, the Marble cloud service includes patented, adaptive protection to eliminate risks to corporate data, networks and applications. Marble secures mobile workers' access to corporate and public networks and cloud services on Android and iOS mobile devices, as well as Macs and Windows PCs, offering comprehensive protection.

The Marble Security platform consists of three components: Marble Control, Marble Access, and the Marble Network. (Fig. 1)

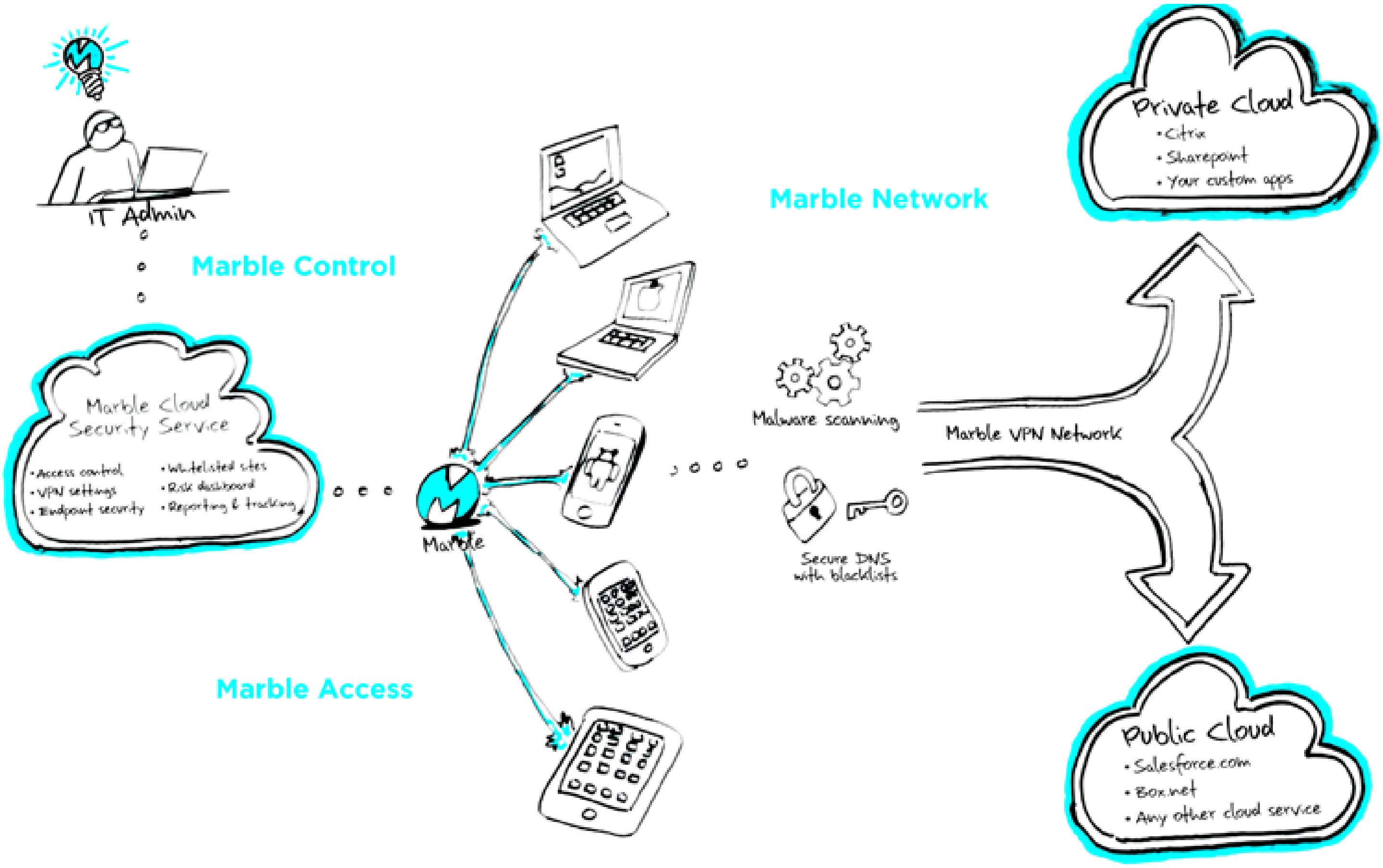

Fig. 1. The Marble Security Service secures mobile workers' access to corporate and public networks and cloud services on Android and iOS mobile devices, as well as Macs and Windows PCs

Marble Access: Employees download the Marble application onto whatever device they intend to use to access the company network: a PC or Mac, as well as their Android or iOS devices. For Android devices, the Marble app is available from Google Play; for iOS devices the app is offered at the Apple App Store. For the Windows and the Mac OS platforms, the end user may download the application onto their computer from an email link that's sent by an IT administrator. Once the user registers the application, that endpoint becomes intrinsically bound to your management service, offering administrators control over risk and the device.

Marble Network: The Marble Network is a purpose-built private network that allows IT to either move traffic through their own VPN service, or use Marble's own VPN network. If a company has its own VPN infrastructure, it's possible to imbed its VPN client within Marble's client. If your enterprise is without a VPN infrastructure, the Marble VPN can be used by itself with complete security and confidence. Users can then securely access private cloud data that sits behind a firewall, such as Citrix or SharePoint, as well as public cloud services like salesforce.com and box.net.

Marble Control: By logging into the administrative control center, IT can set policies, run risk reporting, and access a rich dashboard to track which employees have devices, the devices used, applications, and data downloaded. From that management console policies for privacy and passwords can be set, and devices provisioned and de-provisioned.

The Marble Network offers mobile workers:

- Isolated web browsing: On PCs and Macs, virtualization technology provides a read-only browser invulnerable to malware. For iOS and Android devices, a secure browser provides a protected environment where personal data is never stored on the device so it can't be stolen or leaked.
- Secured encrypted connections: Protects online sessions from crimeware and network attacks from a virtualized workspace to inside the firewall.
- Verified web destinations: Secure DNS look-up prevents browser redirects from poisoned DNS and other threats.
- Site access control: Blacklists and whitelists prevent visiting malicious sites to protect against phishing and malware attacks.
- Data loss prevention: Policy management by user, device and content to control copying, pasting, and printing over the network.

- Compliance and risk management: Built-in password protection and management, content loss prevention, and centralized control over remote devices helps reduce risk and achieve regulatory compliance.
- Password protection and management: Protects against phishing scams and re-direct attacks using real-time website blacklists and whitelists.
- Unifed user experience: Works similarly across all devices, with the same interface for desktop and mobile devices, regardless of platform.

Conclusion

Hackers, hacktivists and hostile governments use a multitude of strategies to steal corporate information, break into online accounts and humiliating government agencies and businesses. These criminal organizations' sophisticated and persistent attacks against corporate networks invariably begin by stealing credentials from an employee's computer or mobile device. When employees access the network from a device they own, beyond the control of IT, the risk is far greater and represents the weakest point in the enterprise network.

While no single solution can possibly protect against the constantly changing and vast number of cyber threats against business and government, IT can better protect the mobile devices and computers used by mobile workers. Until now, CIOs were required to cobble together numerous solutions to fend off threats to these employee endpoints.

Marble Security provides a single, comprehensive service that protects against the array of threats to mobile devices. By harnessing virtualization technology, tracking, network security and DNS security, Marble reduces the risk of attacks to enterprise networks.

For more information, or to evaluate the Marble Security solution, call 855.737.4373 or email sales@marblesecurity.com.

Marble Security, Inc., offers a mobile security cloud service that protects against the ever-changing threats being unleashed into enterprises by mobile devices. Simple to use and deploy, the Marble cloud service includes patented, adaptive protection to eliminate risks to corporate data, networks and applications. Criminals, competitors and hostile governments are targeting enterprises and end users with an ever more sophisticated array of attacks. The BYOD workforce is particularly at risk. Marble secures mobile workers' access to corporate and public networks and cloud services on Android and iOS mobile devices, as well as Macs and Windows PCs, and offers more comprehensive protection than any other solution on the market.

Contact a security specialist:
T: 855.737.4373
E: sales@marblesecurity.com

MARBLE

Marble Security, Inc.
600 West California Avenue
Sunnyvale, CA 94086

T: 408.737.4300
Toll Free: 855.737.4370
Fax: 408.737.4301

www.marblesecurity.com