



Whitepaper

2011

A Heuristic Approach to Mobile Security

A J.Gold Associates White Paper

“There is a dramatic shift taking place in many organizations as the role of mobility becomes more pronounced and achieves more diversity. This “consumerization” of mobile computing has made the traditional corporate dictate imposed on its users of obtaining only company-approved devices obsolete. But despite this end-user-driven mobile device liberalization trend, organizations must still maintain and manage corporate security and information integrity. And they must do so even when personally chosen devices may not be fully up to the task... few companies currently have systems in place that can handle this challenging paradigm shift.”





Contents

Introduction 2

The New Reality in Enterprise-Class Mobility..... 3

New Devices, New Exposures 3

Implementing a Layered Approach 3

What Kinds of Security Issues Exist?..... 3

What Does a Lost Device Cost an Organization?..... 4

 Figure 1: Mobile Devices Lost per Year 4

 Figure 2: Average Cost per Lost Device 5

Defining an Enterprise-Ready Device 5

Enhancements are Often Needed..... 6

A New Approach to Security Management is Required..... 6

A Contextually Aware, Dynamically Adjusted and Heuristic Approach 6

Dynamic Monitoring and Adjustment 7

 Figure 3: Dynamic Monitoring Points Affecting Policies..... 7

Moving from Static to Dynamic – A Checklist 9

 Figure 4: Checklist for Current vs. Next Generation Device Security Management 9

Conclusions..... 9





Introduction

There is a dramatic shift taking place in many organizations as the role of mobility becomes more pronounced and achieves more diversity. In the past mobile devices were specified, deployed and managed exclusively by the IT department with little to no input from end users or even line of business managers. But in the past 1-2 years, we have seen a markedly different dynamic with the emergence of popular consumer-oriented smart devices. There is overwhelming user demand to employ a variety of device models and types, including personally chosen and acquired devices. And with such demands often coming from within the executive ranks, IT is forced to react and integrate them into organizational systems. Further, many users regularly employ 2-3 different mobile devices, making IT's task even more difficult.

This “democratization” of mobile computing has made the traditional corporate dictate imposed on its users of obtaining only company-approved devices obsolete. Choice is becoming the norm. But despite this end-user-driven mobile device liberalization trend, organizations must still maintain and manage corporate security and information integrity. And they must do so even when personally chosen devices may not be fully up to the task.

To further emphasize this rapidly changing environment during the next few years, we highlight one of J.Gold Associates' key Emerging Trends:

- ***The advent of consumerization of IT, bring your own device to work, and the renewed power of the end user to determine strategy will force corporate IT groups to dramatically alter their function. By 2013-14, those corporate IT departments who have not enabled a diverse population of devices and end user choices through emphasis on manageability, policy enforcement and security evaluations will become hopelessly outmoded and struggle to function. This will cause chaos and substantially raise the TCO of the organization.***

Companies must embrace this changing dynamic, but must do so in a way that will maintain access and information security, allow effective mass deployments to large numbers of users on different device types and form factors, ensure effective management and support of those devices, minimize cost of operations, and maximize ROI. This is no small task given the lack of homogeneity in device attributes and capabilities. The way of uniformity and of a single device and/or user model no longer works. And few companies currently have systems in place that can handle this challenging paradigm shift.

This paper will address the aspects of a new approach to mobile security management that we believe is imperative if organizations are to keep up with the fast pace of change in mobile user demands and devices.



The New Reality in Enterprise-Class Mobility

The world of mobile workers and devices is changing. In fact, the rate of change is often overwhelming, with new devices, features, form factors and connectivity options becoming available almost continuously. No longer are typical device lifetimes measured in years. Rather, they are often being measured in months. New and desirable form factors (e.g. tablets) features (e.g., multi-touch screens) and functions (e.g., apps from app stores) are delivered to consumer devices well before they are available on traditionally enterprise-targeted devices. It is this “consumerization” of mobility that has driven end users to demand more compelling choices in mobile devices at work, and consequently forced organizations to adapt to this change. Indeed, the line between a consumer-grade and enterprise-level device is far more “gray” today than it was a few years ago.

New Devices, New Exposures

With the emergence of increased use of mobility and more diverse mobile platform choices, organizations have been left more far more exposed to security failures. In the past companies chose a single defined platform which was locked down and secured. As a result, most users were “locked out” of deploying any devices that were not corporate supplied and/or approved, which usually meant the majority of new, feature-rich and popular devices (e.g., iPhone, iPad, Android). Users are now demanding (and getting) next generation and often consumer-oriented devices. As a result, the number and types of security and policy breaches is growing. Organizations are now struggling with what needs to be done to make these devices secure and enterprise-ready.

Implementing a Layered Approach

To truly secure the organization against the increasing variety of mobile-centric threats, a layered approach is required. This includes not only maximizing the security inherent in the device natively or through supplementation (e.g., encryption, authentication, malware protection), but also by creating protected access through any entry points into the organization (e.g., VPN, encrypted networks). And no security layering can be complete without a policy enforcement capability that implements controls based on real and/or perceived risks. Policies should be based on the characteristics of the device, user type, connectivity needs and application requirements. It is only through a layered approach that “encircles” the organizational securely in multiple layers that the maximum amount of threat prevention can occur, especially given the nearly continuously changing nature of mobility.

What Kinds of Security Issues Exist?

There are a number of real security challenges facing companies with the expansion of mobile device numbers and proliferation of device types. Recent examples of mobile security failures include:

- iPhone “rootkitting” that allows bypassing of security
- Android malware capturing device information and forwarding to web site
- Loss/theft of highly portable (and unprotected) tablets and/or smartphones



A Heuristic Approach to Mobile Security

- “Spoofed” ActiveSync policy app on Android which reported higher security than was actually available
- “Co-mingling” of user data and corporate data
- Ease of Copy and Paste to retrieve and re-transmit sensitive information
- Beginnings of true malware (similar to PCs) that steal data and affect other devices
- Unchecked access to apps within App Stores that include malware

And the number and associated cost of security lapses will certainly increase with more powerful and more memory-rich devices that access corporate apps and sensitive data.

What Does a Lost Device Cost an Organization?

It is estimated that approximately 5%-10% of laptops and 15%-25% of phones are lost or stolen each year. So a company with 5,000 users will lose 250-500 notebooks per year, and 3-5 times that many phones. While no data yet exists for tablets, there is no doubt a significant number will be lost or stolen (we estimate in the 10%-20% range). And with smartphones and tablets often containing 32GB to 64GB of on-board memory (and more with removable flash memory cards), the potential amount of sensitive corporate data that could be compromised is substantial.

Figure 1: Mobile Devices Lost per Year

Mobile Devices Lost per Year	%	Number*
Phones	15-25	750-1250
Notebooks	5-10	250-500
Tablets	10-20	500-1000

**Number based on organization with 5000 users*

Copyright 2011 J.Gold Associates, LLC.

The replacement cost of the lost device is trivial but the cost to an organization to mitigate any data loss can be staggering. The Ponemon Institute, in a recent study (March 2011), indicates that it costs a company \$258 for each exposed record to remedy the failure. Losing 10,000 records contained on a missing device will cost the organization \$2.58M to rectify. There is no doubt then, that making the myriad of consumer-focused devices coming into the organization enterprise-secure can have a huge Return on Investment (ROI).

While the number of data records on each device will vary by company size, user class, industry, etc., it is not unreasonable to assume that a notebook could easily store 10,000 personal and/or sensitive data records – a number that is significantly smaller than many of the publicly reported high profile notebook loss cases. We estimate the average data record numbers for smart phone devices at 5% of notebooks (500) and for tablets at 20% of notebooks (2,000). At \$258 per record, the average lost notebook will cost \$2.58M, the average lost smartphone will cost \$129K, and the average tablet \$516K to remediate.



Figure 2: Average Cost per Lost Device

Average Cost per Lost Device	Records	Cost*
Phones	500	\$129K
Notebooks	10,000	\$2.58M
Tablets	2,000	\$516K

*Based on number of records times \$258 cost per lost record

Copyright 2011 J.Gold Associates, LLC.

Breaking the Law?

While costs to remedy data exposure can become staggering, it is also important to note that most organizations must also abide by governmental regulations. Compliance failures can not only result in substantial fines, but in some cases can even result in executives being arrested. Some of the regulations that organizations need to comply with include:

- Sarbanes-Oxley Act (US)
- Gramm-Leach-Bliley Act (US)
- Health Insurance Portability & Accountability Act (HIPAA) (US)
- FDA Title 21 (US)
- European Union Directive (EU)
- Euro-SOX (EU)
- CA Senate Bill 1386 (US)
- Payment Card Industry Data Security Standard (PCI) (US)
- Personal Information Protection & Electronic Documents Act (Canada)
- Data Protection Act (UK)

Nearly all businesses are affected by one or more of these regulations, and the number and scope of regulations is expected to grow as numerous Federal, State and International initiatives are underway that will increase required compliance. Organizations must create a strategy to deal with compliance or face potentially business-threatening penalties.

Defining an Enterprise-Ready Device

There are a number of features that set apart an enterprise-ready device from a purely consumer level device. Included in this list are features such as:

- Ease of provisioning and mass deployment
- Ability to set policies for features/functions and users
- Secure connectivity via VPN
- Synchronization with Email (typically with Exchange via ActiveSync)
- Device Lock/Kill
- Secure login and enhanced authentication
- On board encryption for data at rest security

All of the above features/functions should be available through a method of automated policy enforcement so that corporate IT can have ultimate control over the device. Many consumer level devices are not enabled with remote policy setting features, and provide only for end user settings. Some may even allow end users to override IT defined policies. It is not



A Heuristic Approach to Mobile Security

possible to achieve adequate organizational governance if any policies can easily be modified or undone by the user.

Enhancements are Often Needed

Most consumer-level devices can't meet these criteria without having additional software installed, including many of today's most popular devices. It is therefore imperative that any devices not up to the task be supplemented with enhancements that make the device as close to the desired enterprise level as possible. Alternatively, those platforms that can not be made fully enterprise-ready can still be used in limited situations. However they must be controlled and managed so that some level of reduced functionality is available to the end user without compromising the organization. This will vary by platform, OS, form factor, manufacturer, etc. To address these challenges it is imperative that corporate mobile infrastructures compensate for vulnerabilities by implemented a solution that enables IT to securely monitor and manage not just the devices but also access and network connectivity.

A New Approach to Security Management is Required

Because of the growing diversity in platforms, and the inability to define a universal set of policies that can be easily and cost effectively managed by IT, mobile security management must transition from its currently device management focused model to a more comprehensive dynamic and heuristic approach – adapting dynamically for device type and usage requirements. This is the best way to rationalize the needs of the organization for cost-effective and secure control with the desires of the user community for open choice in device type and functionality. Device management is a valuable but limited first step. We need to evolve to a higher level of management capabilities that encompass the entire mobile ecosystem.

A Contextually Aware, Dynamically Adjusted and Heuristic Approach

Adopting a dynamic policy-based enforcement model provides many benefits to the organization including:

- A variety of devices and user types can easily be integrated into the organization without compromising security management.
- The total cost of ownership can be controlled and not spiral beyond reach, which is often the case with a non-uniform approach to device management.
- User desires can be accommodated (within certain boundaries and constraints) without adding to the workload and stretching the limited resources of IT.
- Companies have a new flexibility that allows them to move with the market and adapt to new devices and usage models without undue costs or hardship.
- Users will have the flexibility they demand in choosing and deploying a wide variety of user furnished devices, and upgrading them as desired.

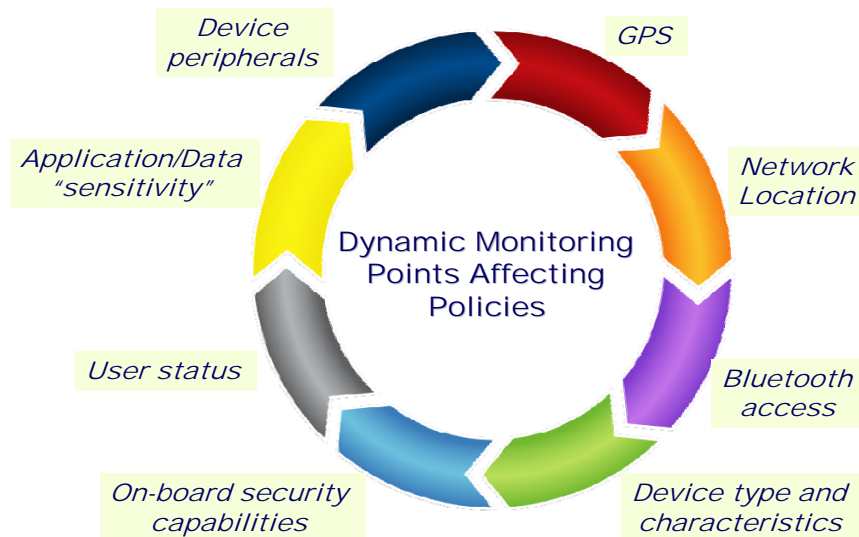
All of this means that current generation fixed-function mobile device security management solutions are rapidly becoming outmoded and obsolete. Indeed, the next generation of these products will encompass a number of critically important and unique features.



Dynamic Monitoring and Adjustment

A contextually aware heuristic based approach dynamically alters any set policies for manageability and security based on key attributes at the time of use. This is a significant improvement from the static policies that most device management products currently create and enforce. A typical set of determining factors in HW, connection and usage for dynamic policy setting are highlighted in Figure 2.

Figure 3: Dynamic Monitoring Points Affecting Policies



Copyright 2011 J.Gold Associates, LLC.

Below we further describe the required monitoring points that must be evaluated to provide contextually aware managed security and policy enforcement.

- **GPS** – To optimally set the policies of a device, location can be an important factor. For example, knowing a device is located within the company campus and attached to the corporate network (and not on a public network), will have an effect on the security of the device. Further, knowing that a device is not local, although it is supposed to be, could indicate that the device has been lost or stolen and could trigger a lock or kill operation. As nearly all mobile devices now have GPS (or can be located through network access points) location becomes an important determinant in setting a usage policy for the device and the user on a dynamic basis.
- **Network Location** – Like GPS above, network access location should be a factor in dynamically setting a policy for both the device and user. Devices connecting to corporate resources from an unsecured network should have specific policies enacted to require enhanced security (e.g., VPN) to prevent unauthorized interception. Further, network characteristics (e.g., speed, latency) can be used to provide feedback to application use (e.g., disabling video on a slow or expensive-per-MB network connection).



A Heuristic Approach to Mobile Security

- *Bluetooth access* – Network connected peripherals and “phishing attacks” can expose the device to infiltration and damage. Because of this, the Bluetooth network should be subjected to control mechanisms. This is often overlooked as an exposure point by organizations and should become a component of mobile security management.
- *Device type and characteristics* – Not all features and functions on a device are appropriate for all classes of workers (e.g., camera, media player, browser). Further, network access, screen type/size and even messaging access/capabilities may vary by device and worker type. The ability for a company to lock, limit or disable features and functions enhances security, lowers risk, and can even lower the TCO.
- *On-board security capabilities* – The types of applications allowed, availability of connection to the corporate network, and the amount of data allowed to reside on the device should be configurable based on the amount and quality of built in security inherent in a particular device (e.g., HW enabled encryption, enforced VPN connections). There is a relatively high amount of variability between devices, and the ability to dynamically set the correct user access based on an understanding of capabilities is imperative to secure corporate data from loss and/or being corrupted.
- *User status* – The user status should be included in assessing the level and type of connection to allow, and the data to be accessed. What is the user level in the organization (e.g., CxO, staff member)? Is the user traveling? What time of day is it (e.g., is it after work hours which could indicate a misuse or lost device)? These factors can be used to provide access to certain applications but not others. They can also be used to enable or disable certain features/functions on the device (e.g., automatically setting WiFi network to on when in the office, restricting web browsing to reduce data usage when travelling and connected in a roaming environment).
- *Application/Data “sensitivity”* – The type and amount of data to be accessed can be used effectively as a key contributor to dynamic policy enforcement. Some data accessed by users is of relatively lower value if lost. However, if it is financial or personal data (e.g., credit cards), or corporate sensitive documents, then enhanced policies are implemented for user access of the data. Sensitivity of the data should be a key determining factor in which devices can access the data, and what remediation (e.g., VPN, encryption) must be enabled before the user can gain access to the information, network or application. Further it can be used to allow or prevent transfer of the data onto the device, or lock out the device if it’s determined to be attempting to access the data in an unauthorized fashion.
- *Device peripherals* – If in the normal course of work the user has access to and requires the connection of peripheral devices (e.g., printers, scanners), it could be important to note the absence of such peripherals as it could affect the ability of the user to be productive, and could also be an indication that the peripheral has gone missing. This can help with anti-loss initiatives in those organizations that may need to control auxiliary devices. The ability to dynamically disable the device and/or peripherals, making them useless without the proper connected/docked device, would make theft of peripheral devices much less attractive.



A Heuristic Approach to Mobile Security

The above represent important contextual points that should be incorporated into policy setting, but may not be representative of all possible contextual points. Companies will often “learn” through experience which criteria are the most critical to monitor and use most effectively, and which policies can be dynamically altered with least disruption to users and corporate apps. This will ultimately be accomplished through monitoring of their effectiveness in various situations. Heuristically enabled security management should be expandable to include required criteria for unique capabilities, new usage models, or as more features/functions become available on the device. Learning what policies are needed, and easily adding them if not already available, is a key component of the next generation of mobile device security management tools.

Moving from Static to Dynamic – A Checklist

It is important that organizations rapidly move towards the next generation capabilities in device security management. It is the only way they will be able to keep up with the rapid pace of change of mobile platforms and user demands for new ways to use the devices. Below we provide a brief checklist that highlights some key differences to evaluate in looking at current generation vs. next generation products.

Figure 4: Checklist for Current vs. Next Generation Device Security Management

	Current Gen	Next Gen
Device flexibility/adding new device types easily	+	++
Threat analysis and ease of updating	-	+
Location aware usage model	-	++
User device switching capability	+	++
Device capabilities knowledge base and policy adaptation	-	++
Network security aspects of connection types and locations	-	++
Dynamic corporate policy enforcement vs. fixed set-up	-	++
Scalability/Expandability	+	++
Application/Data Security	+	++

Copyright 2011 J.Gold Associates, LLC.

Conclusions

There is a dramatic change taking place in mobile devices and usage patterns, one which most enterprises currently have trouble coping with. The need for mobile security management has never been greater, yet many current generation tools to aid in this process are lacking completeness. Companies must adapt and deploy policies that can secure their corporate assets while keeping costs low and keeping end users engaged. To do this, a new generation of automated, heuristic and dynamically adjustable mobile device



A Heuristic Approach to Mobile Security

security management products must be deployed. Without the needed improvements in managing the increasing diversity of devices, connections and usage models, most organizations will be left struggling to keep up, and ultimately be left unprotected. Organizations must create a strategy in the short term that will address the changing dynamics and protect their assets while keeping costs low, allowing IT to maintain oversight while staying within its limited resources, and enabling end users to choose their preferred device. Without this, companies will be forever playing catch-up to the market, negatively affecting cost of operations and overall productivity.

About J.Gold Associates

J.Gold Associates provides insightful, meaningful and actionable analysis of trends and opportunities in the computer and technology industries. We offer a broad based knowledge of the technology landscape, and bring that expertise to bear in our work. J.Gold Associates provides strategic consulting, syndicated research and advisory services, and in-context analysis to help its clients make important technology choices and to enable improved product deployment decisions and go to market strategies.



J.Gold Associates, LLC
6 Valentine Road
Northborough, MA 01532 USA
+1 508 393 5294
www.jgoldassociates.com