The BYOD Mobile Security Spectrum: A Taxonomy

By Winn Schwartau
The BYOD Mobile Security Spectrum: A Taxonomy
By Winn Schwartau

“To BYOD or not to BYOD?” is the question that just about every private, government and military organization is asking itself today about the consumerization of IT by mobile devices of myriad flavors.

I, however, do not believe that the BYOD conundrum is an ‘either-or’ binary question. The mis-phrasing of the question itself has been cause for much industry confusion, thereby limiting the organization’s real spectrum of options for securing the mobile enterprise.

Creating a taxonomy is a tricky business in which I have had some past success. The industry has no prior-works on the subject (for many reasons, including a lack of vendors with deeply entrenched security experience), so I will attempt to functionally taxonimize the security spectrum of BYOD options available to the enterprise today. That being said, I welcome constructive debate and criticism so that the BYOD Mobile Security Spectrum can be enhanced and updated in the future.

Do Nothing

It is absolutely astounding how many organizations, of all shapes and sizes, in every imaginable industry sector have been caught with their mobile pants down. Surveys tell us how many companies do not even know what mobile devices are connecting to their network, their intranet and resources.

CISOs, CTOs and CIOs have openly cringed in my presentations around the world when asked, “How do you currently control devices, access and data in your mobile work force?”

Many of us come from the BlackBerry standard where we didn’t have to think about security. It was built-in, as it should be, into a locked-down device, and management was handled invisibly in a data center with a BES, Blackberry Enterprise Server, far, far away. No matter how unappealing and risky the ‘Do Nothing’ BYOD option is, it will be with us for quite a while.

MDM

MDM is a lawsuit waiting to happen.

In June 2007 with the introduction of the iPhone, we saw the term MDM – Mobile Device Management – added to the lexicon. Unfortunately, with a lack of technical acumen, the media and many analysts got stuck on this new acronym, and it has too often inaccurately been used synonymously with mobile security. Nothing could be farther from the truth.
MDM is not security. Yet, at last count there were something like 80 MDM-only vendors, some of whom, more than others, are falsely positioning their MDM products as an adequate mobile security solution for the modern enterprise.

It is my belief that the regulatory compliance industry will send the Grim Reaper to the doors of many enterprise MDM users. As regulated data is moved to, stored on and accessed from mobile devices, organizations cannot ignore compliance adherence. Those that chose to do so, either by ‘Doing Nothing’ or implementing anemic ‘MDM’ as poor-man’s security, will significantly increase their odds of being targeted by the wrath of the legal system and regulators sensitive to public privacy protection failures.

Someone, some large high-profile company is going to get sued in a big way when a data leak, breach, mobile hack or external mobile system penetration occurs. Then it will be disclosed that instead of echoing the strength and stringent security controls they use in their fixed enterprise, they chose to ‘cheap-out’ with an MDM product. Embarrassment, humiliation and technical ridicule will follow levied fines and expensive breach notifications due to a failure to use Best Practices.

Many organizations, initially under the belief MDM tools alone would meet their security needs, are already discovering the cost and pain of dismantling their inadequate MDM approach in favor of deploying more comprehensive mobile MDSM (Mobile Device Security & Management) suites.

**Sandboxes, Containers & Wrappers**

The concept for this kind of BYOD implementation is simple, but in my opinion, not a viable long-term security approach. Sandboxes and containers are no more than mobile apps that the user must invoke to use. These new apps, first of all, change the entire user experience which was the initial attraction to the consumerized mobile device to begin with. This means user training and support time and expenses for the sandbox app.

Beyond that, though, lies a core hurdle: how easy is it to build a full featured browser? Every security professional understands the problems therein, and a sandbox BYOD approach complexifies the problem with yet another browser. Further, a new email client must be designed and integrated, that may or may not have problems integrating with widely deployed mail servers and its own set of additional security weaknesses.

Sandbox BYODs may have further security deficiencies if the goal is to provide the mobile user with access to corporate resources and data. Administrators need to understand how the specific access controls are designed, vetted and applied, and then if and how they can be tied to existing firewalls or other ACLs.

As I believe in ‘Defense in Depth’, sandboxes represent to me a potential single point of failure. With hostile groups aiming at the mobile user more and more, at what point will the sandbox – or container’s walls – be breached? Memory isolation techniques and virtualization can be valuable tools in a controlled environment, but I am yet to be convinced that they do not suffer from a sense of bravado.

A mobile environment by definition is more hostile, and if a vendor’s memory protection schemes are weak or subject to a vulnerability caused by an OS vulnerability (known or not), the entire mobile defense collapses. Given that so many companies are having severe problems with containers and sandboxes, it’s worth a careful look to see if this approach really works for the organization.
I also put app-wrapping into this section of the spectrum because it is highly focused on protecting specific apps with VPN capability rather than the entire device. For custom apps, wrapping is a good approach, however, its real strengths become apparent under Mobile Device Encryption.

Not surprisingly, though, a little research will show that many top notch organizations are viewing that the lesser security oriented BYOD solutions are in fact more expensive that doing it right. So, one has to consider the wisdom of the last thirty years of security: if you are bolting on security as an after-thought, and it costs more in the long run with a true TCO (Total Cost of Ownership) analysis...why are you bothering? My experiences over the last several years suggests that such non-best-practices decisions are made by non-technical, non-security people, who believe the false promises of limited mobile security efficacy.

**MDSM-1: Mobile Device Lock-Down**

Mobile Device Security Management adherents take a much different view of mobile security.

As RIM's BlackBerry has rightfully done for years, effective security control begins with device lock-down. Device-identity authentication, such as using a CA-based handshaking schema in conjunction with AD is essential to create a reliable basis for mobile work-force provisioning, management and reporting.

But perhaps more importantly as part of the lock-down initialization, is the security enforcement of an always-on VPN, to ensure that all traffic in and out of the mobile device meets industry best practices. A centrally managed VPN not only insures that carrier data traffic is protected but three significant positive benefits result:

1. VoIP traffic becomes encrypted, enabling a native secure voice channel for mobile phones.
2. WiFi traffic is now encrypted, enabling transparent and secure use of Hot Spots anywhere.
3. The user cannot bypass the VPN.

Since SSL-based VPNs have known vulnerabilities, the industry, as aptly demonstrated in the 27 February 2012 NSA document, "Mobile Capability Package" will necessarily adapt iPSec VPNs (at least 256 bit AES, perhaps FIPS 140-2/3) as the default minimal standard for mobile VPNs. At this point, I believe that anything less than an always-on VPN, such as native SSL, will not be regarded as Best Practice.

Optionally, though, some organizations may, for many reasons, elect to allow some device traffic to be transported through a personal email server. The aim here is to alleviate concerns on the part of the user that his personal emails can be read by the company. Applying a split VPN for such cases should be an integral part of any mobile implementation to give administrators both current and future security control and flexibility.

**MDSM-2: Mobile Content Control**

Does any organization want adult materials to appear on its computers or mobile devices? What about access to gambling or hate sites? These are policy questions to be sure, but I again fail to understand why an organization would not want to have appropriate controls in place over user activity, Internet and local network resources.

Mobile Content Control begins with a hardened stateful inspection mobile firewall that gives the policy and security administrators the same amount of enforcement control they currently enjoy over the rest of their enterprise, including services, ports, processes and users/groups.
One hugely positive side effect of implementing MDSM-2 level mobile security for BYOD with a centrally managed mobile firewall is that the entire mobile population becomes invisible to the Internet and attackers. The device IP address is removed from the security equation, and the security efficacy is mandated by the enterprise.

In organizations that are mobility heterogeneous, policy enforcement can be further granularized by Device Type and User Risk. Androids and iDevices have different native capabilities and control attributes, thus the risk is different. In the chart below, we have three types of devices: iDevices, native Android with limited MDM controls and a Kernel modified Android giving highly granular administrative controls over the device itself.

Users come in different flavors, too, from the C-Level to the lowest rung on the ladder. For each group, there is the question of “How Much Do I Trust Thee?” and how much access that group or class of device is going to be given to network resources and data.

This example shows how some of this ‘Device Type’ policy enforcement would look, mapped across user groups and access rights. MDMs only provide binary access control to the network (notably flat ones) – it’s all or nothing. Ergo, the need for dynamic resource access controls through administration and policy – just like it is done in our fixed enterprise networks.

An oft overlooked attack vector and potential high risk to mobile enterprises is email. What reason is there not use anti-virus and malware controls over email to the mobile device? The industry currently has a small inventory of known hostile mobile-specific signatures, but more than 600 million unique pieces of malware have been identified to date, increasing at a rate of almost 30 million per month. For MDSM-2, some basic app black listing should be included, and enhanced as reputation engines evolve.

Finally, attempts to compromise the mobile device, such as through jail-breaking, must be detected with such speed that an automatic remediation can be initiated so that data breaches or damage(s) are immediately mitigated. We successfully use IDS and IPS in the enterprise, which provides us with the evidence to support that these capabilities are necessary for all mobile enterprises, too.

Security has evolved to a defense in depth mindset and the same thinking should apply to mobile security implementations. MDSM should be designed in such a way that allows the rapid seamless integration of additional security tools into the BYOD security controls suite.

Some companies may choose to add higher levels of granularity for web filtering, while others may care less, or otherwise choose broader policy blocks to be enforced at the centrally managed mobile firewall.

Many companies have chosen to further extend their mobile security with the inclusion of DLP and SIEM, both for clear reasons to the security practitioner. MDSM-2 level security should offer both the tools and the ability to integrate into existing DLPs and SIEMs, extending the controls to the organization’s entire mobile enterprise.

Since apps are (arguably) “the most efficient malware distribution system ever invented by man,” a distinction between public app stores and private enterprise app stores must be part of any strong mobile security effort. The differences between the Apple App Store, Android Marketplace and countless unapproved app download sites are profound. But even more profoundly, unless apps are completely vetted with a formalized code review, there is every chance that an approved app may well become hostile via either event or time triggers secreted into the binary.

App stores cannot, do not, and should not be expected to provide that level of scrutiny. Therefore, additional alternative methods of analysis are required. A combination of app filtering and ABC (Application Behavior Control) provides the best of breed methodology. Rather than relying upon static code imagery in the hopes of identifying hostile ‘DNA’, a dynamic application behavioral based control system is the preferred method.
In both iOS and Android, there are unacceptable behaviors such as reading or writing to system-only memory locations, PII access and a dozen or more actions that violate good security, privacy and compliance guidelines. A well-constructed ABC mechanism will always be active (with no need for resource intensive background tasking), capable of being updated on-the-fly and initiating high speed remediation.

**MDSM-3: Mobile Device Encryption**

Device level encryption to protect data at rest is certainly kernel and OS dependent, and their approaches are substantially different. In a non-multi-tasking environment this is very difficult to do, especially one that does not natively offer a modified kernel designed to implement this level of security. Android and iOS take different approaches, and the flexibility to perform and deploy kernel modifications that iOS users and enterprises cannot take advantage of.

For BYOD, some organizations find that MDSM-2 meets their Best Practices requirements, especially those that do not allow sensitive data to reside at rest on the mobile device. That may mean using a Citrix-like tool to access corporate resources and essentially treat the mobile device as a fancy GUI cum dumb terminal; albeit one that is locked-down with encrypted traffic, firewall controls and filtering – all necessities no matter which BYOD method is preferred.

Applying another level of defense in depth is achieved by adding a Container along with selective app-driven localized encryption. As described earlier, ‘App Wrapping’ provides trusted app download mechanisms in addition to specifically designed functionality that requires an extra layer of security.

Keep in mind, though, that even if your users are operating under the invisible security shells of lock-down, VPN, firewall and content filtering controls, there are downsides. Any additional container must be invoked, the user must authenticate to it and learn how to use it. Further, given the background tasking limitations of non kernel modified Androids, the usability of such a container may be functionally limiting.

The use of virtualization in any aspect of BYOD does add a level of complexity and potential for failure. But if the VM or Hypervisor based container is maintained under a proper shell of security (defense in depth again!), at least a failure of the VM or container does not expose the entire device or its data to compromise.

**MDSM-4 Geo-Location Policy Enforcement**

Mobile devices are... well, mobile. Yet, too few organizations have chosen to implement Geo-Location Policy Enforcement. (Some use the term Geo-Fencing.)

For example; if your company does business in some culturally sensitive region of the world, it might be best for you and your company’s relationships, to be more restrictive with firewall, content filtering and other security enforcement policies. Thus, when a planes lands, say in the Middle East, perhaps all adult materials are made inaccessible.

In China, perhaps, any links or communications with those resources deemed politically improper should be filtered out. With mobile firewalls and filtering capabilities, applying such dynamic rules makes mobile devices truly mobile, yet also reduces the risk of ownership and data breaches.

Or, perhaps healthcare workers need one set of enforcement while at work and another when away. Should trading floor rules be the same as when out and about? What about government and the defense establishment? Geolocation offers great power over access rights in a mobile environment.

Geo-location policy enforcement comes in two fundamental forms.

1. GPS or tower-based resolution enforcement is more than enough for many organizations. With a policy enforcement resolution of approximately one mile, a mobile device can be transformed from a business to a personal device when someone leaves the office, thus creating a spatial differentiation for BYOD implementation.

2. More organizations are extremely security sensitive than you might think. By integrating a set of sensors with the mobile firewall and policy enforcement capabilities, a highly granular resolution of 3 meters can be achieved. The device policy changes from office to office, floor to floor or as otherwise arranged. From financial institutions, medical facilities and government and military installations, security needs and controls can substantially vary from ‘door to door’ and mobile security should be able to effectively enforce such policy, automatically and invisibly to the user.
**Air Gap**

Then there is the air gap, the antithesis of Doing Nothing and the most secure end on the Mobile Security Spectrum.

With Air Gap, users have one mobile device for business and an entirely separate one for work. It initially costs the company a bit more than a mere monthly stipend to the employee, but is the risk of BYOD worth it? Again, recent findings suggest that BYOD is more expensive than maintaining two devices, one under complete corporate control.

Androids and iOS can be made as secure as a fully compliant desktop computer, but it is the BYOD conundrum that adds so many variables, introducing risk to all parties.

Each company needs to decide its own risk and pain tolerance. Someone is going to get sued, and we do not yet know the strengths or weaknesses of BYOD in a legal contest. On the other hand, we do know that for many years, best industry practice was to have a BlackBerry on one hip and an iPhone on the other. Why should we change that model?

**What’s the Right Answer?**

All mobile enterprises present additional risk.

The legal system in untested.

Does personal privacy trump corporate data security? Or is it the other way around?

If I had my choice for the ideal mobile security solution it would look like the following:

1. Air Gap. Two devices.
2. I want my mobile work force as homogenous as possible. iOS plus a select best of breed Androids.
3. Lock-down, VPN, firewall and content filtering.
4. Geo is only necessary for some businesses, and less so in a non-BYOD environment.
5. FDE.
6. Use a Citrix-like remote access tool and minimize any local data storage at rest.

It all comes down to risk, budget, and politics with employees, technical know-how and a willingness to do what is right for the organization.

As the creator of 'Time Based Security', I do tend to add that extra dimension when thinking about security controls and functionality. I see today, too many people only thinking of today, today’s devices, and the apparent needs for today based upon the unpredictable nature of technology and human behavior.

I have to imagine the last thing any enterprise wants to see is the following scenario:

1. Get lots of mobile devices.
2. Oops! What do we do now?
3. No budget.
4. Let’s get MDM. It’s cheap.
Now there's a branching for failure modalities:

a. It just doesn't work.
b. I need more security.
c. I want people to access internal resources with controls in place.
d. Active Sync takes too darned long.
e. What do you mean there's no firewall?
f. Users rebel against non-native experience.

Regardless of the problem, the company is on the same path we experienced decades ago.

1. Uninstall MDM. (That was already paid for.)
2. Downtime and security breaches from mobile workforce.
3. Integrate new MDSM. (More $$.)

This is an initial suite of ideas that will necessarily evolve in the coming months and years. I do invite debate and comment so that I can strengthen the ‘The BYOD Mobile Security Spectrum’.

I look forward to your thoughts.

Winn Schwartau

winn@mobileactivedefense.com
winn@winnschwartau.com