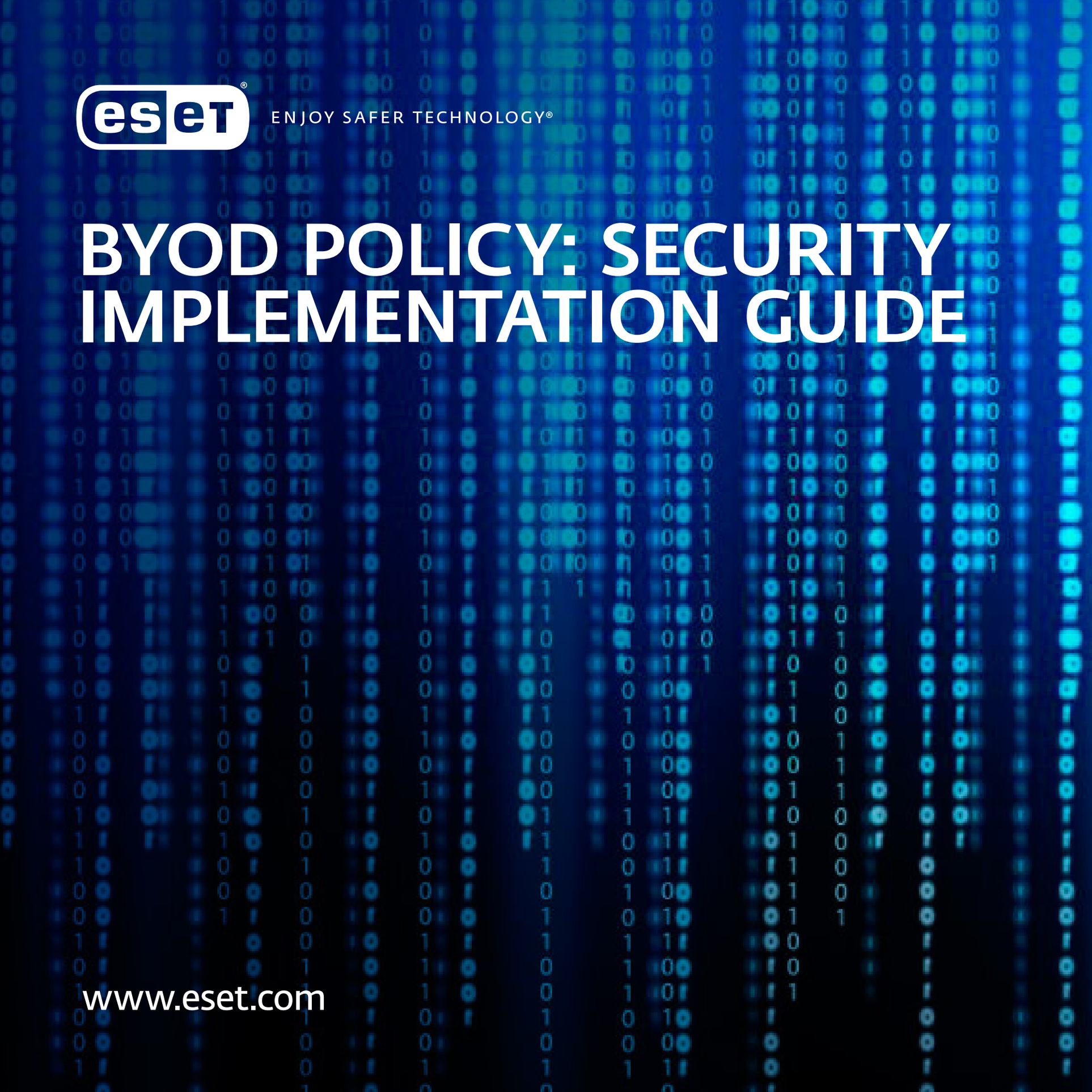
ENJOY SAFER TECHNOLOGY®
BYOD POLICY: SECURITY IMPLEMENTATION GUIDE
www.eset.com

BYOD policy: Security implementation guide

By Michael Aguilar, Business Product Technical Lead, ESET North America

When I was a child, I wanted nothing more than the tablet device that Penny, the character in Inspector Gadget had. You could read on it, use it as a computer, the functionality was limitless. Fast forward to current, I now have that device and it scares the living daylights out of me. How did Penny not get hacked? Did she put tape over the webcam? What OS was that device running to never be affected from outside communications? What protections were or are in place and how can the security holes and threats be mitigated?

Upon getting my first smartphone in 2009, an HTC Hero, I would not have thought that these items would be integrated into the enterprise environment as quickly as they were. The lack of security, infancy of the mobile OS platforms, and multiple vendors seemed to be off putting to many corporate environments where Blackberry OS was preferred with a BES (Blackberry Enterprise Server) server for management. This was the case at my last enterprise site in 2009. Even in 2015, Blackberry was still being praised as one of the most secure OS's, even with their implementation of the *Android OS*. The issue is, no one really uses Blackberry as a personal phone. Most opt for Android (mainstream manufacturers that are NOT Blackberry or Apple phones.)

Combining the fact that phones now have so much functionality, along with a few economic factors, and it almost makes perfect sense to possibly allow your user base to bring their own phones to use at work. The issue you will run into is, with all of the available models, modes, builds, and OS's, how do you possible ensure that the corporate data is protected while allowing the users to be able to USE their phones when needed, even if to play Pokemon GO for a few hours (days or years).

Device management

The first aspect of implementing BYOD is management. You need to be able to manage the devices while ensuring the availability of the overall device if it is not purchased by the company. Whether it is Apple, Android, or other, the primitives are the same, you need MDM (Mobile Device Management).

Apple describes this process of managing mobile devices in an *enterprise environment* as well as a high level overview of the aspects that their *MDM solutions*. Both give advisement on the kind of restrictions and functionality

that can be expected in an enterprise deployment as well as steps to get started with deployment. The *ESET Remote Administrator Server Version 6.3* has the ability to manage these Apple iOS devices through the use of a profile. It can be formatted to restrict certain aspects of the phone for work usage only while also integrating anti-theft functionality in case a BYOD device is lost, keeping your corporate data safe. The setting can be pushed remotely as well, aiding in the ease of deployment.

Android has a multitude of applications that can assist with Mobile Device Management, one of my favorites being *AirWatch*. The containerization that the application uses easily allows it to separate personal data from corporate data, keeping everything segregated for privacy reasons. It can also privatize such data as GPC locations and address other privacy concerns that an employee may have when bringing their personal device into a corporate infrastructure. The downside of this is the large threat landscape of the Android OS. Due to differences in the vetting of applications, Android has a much higher malware rate than Apple devices, therefore an antivirus solution may need to also be implemented to ensure constant protection of a device.

I would recommend the *ESET Mobile Security build for Business*. Not only does it provide antivirus for devices and is manageable with ESET Remote Administrator, but it can also aid in application management, restrictions, viewing of application usage, anti-theft, locking down the SIM card, and much, much more. I had no issues running AirWatch and the ESET Mobile Security applications in tandem on a Galaxy S5 device and Note 5 device. No errors, reboots, or issues incurred.

Testing

After you have decided to progress with a BYOD policy and MDM solution, you will need to test. It will not just be a one install file and complete kind of task. You will want to ensure that your user base has the appropriate access to their full suite of phone applications when not in a corporate setting or on a break/lunch. This kind of aspect will take tuning and trial and error to get the settings to where you allow the maximum functionality along with the highest level of protection. Once everything is validated in your pilot group, you can then deploy controls across the mobile infrastructure to progress with your BYOD deployment. But please, test first, trust me. The last thing needed is a CEO that is unable to play a game or watch a movie at 2am on a Saturday night due to the restrictions you deployed. Been there, not a grand way to spend an evening.

Legal issues

As one would expect, monitoring someone's personal device can prove tricky, to say the least. Get too much information, it is an invasion of privacy issue. If you get too little information, it is basically not much of a solution and will not catch much of anything that would be valuable for you to know or assist with security. This *2013 article from the American Bar Association* has great recommendations about the setting up of the policy portion of your BYOD deployment. Some aspects you want to ensure are:

1. Create a BYOD policy—make it easy to understand, transparent, and detailed enough so the user base understands clearly what will be monitored and what will not be monitored.
2. Educate—teach the clients about the technologies in use and the cope of how they will be used.
3. Get consent—without it you do not have BYOD at your site.
4. Engage the legal department—check with any local or state rules regarding the implementation of BYOD at your business.

5. Containerization—ensure that any remote wipe or data protection features will address the corporate date on the machine while also protecting the personal data, so looking for a solution that provides containerization is best, and I think the end users will appreciate it more.

Starting BYOD can be done quickly however, rolling it out in the correct manner will take time and planning. To ensure the maximum protection of your devices and your business, you will need to ensure that certain validating criteria like legal specifications and the testing of your solutions is conducted prior to roll out. Once the initial framework is completed, you will find it much easier to add onto in the future.

Want to learn more? Check out these 7 quick steps to *mobile device security and BYOD for small business*.

Michael Aguilar is a business product technical lead at ESET North America. He is studying for the CISSP exam and has a Security+ certification as well as a Usable Security certification from the University of Maryland Cyber Security Center via Coursera.org. He is currently responsible for working with large-scale clients for ESET North America and works with ESET developers, QA, and support engineers to resolve issues with clients in a quick and effective manner. Michael is active on Spiceworks and various security forums looking at new threat vectors and the best controls to mitigate those risks.

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.

ENJOY SAFER TECHNOLOGY®