SYNCDOG
WHITEPAPER

For Mobile Security, Antivirus is a Band-aid not a Solution

BYOD 2.0 Via Containerization is the Best Avenue for Greater Mobile Security at the Lowest TCO.

Today, mobile devices are nearly ubiquitous. According to the Pew Research Center, 95 percent of Americans own a cellular device of some kind and 77 percent of that share belongs to smartphone owners. Statista estimates that the number of mobile phone users will surpass the five billion mark in 2019. The vast majority of these mobile device users? Young people. The ones that make up the new work force. It is of natural consequence that the popularity of Bring Your Own Device (BYOD) has increased exponentially in recent years. Enterprise organizations are coming to grips with millennial and Generation Z employees who won't give up their devices or take a corporate-owned without a fight.

A new generation of employees is demanding mobility. More workplaces are offering remote or work-from-home options to their employees, and like it or not, employees are bringing their personal devices into the workplace and using them every day. Even if said employee doesn't access any company files on their device, they are likely connecting to the workplace network, accessing the inner perimeter of your secure infrastructure.

The cost benefits and comfortability factor with a new generation of employees, when it comes to BYOD, make it a great option for businesses keeping their bottom line and employee satisfaction in mind. However, organizations must be cognizant of two caveats when it comes to BYOD – 1) that mobile devices and enterprise systems that manage them were never designed for security, and 2) employee negligence is the biggest threat to an organization's cyber security.

> "Mobile devices are a target ripe for network intrusion and options for detection and remediation remain suspect."

It is well documented that cyber security risks are growing, and this is happening alongside tremendous increase in mobile device use. The result? Mobile devices are a target ripe for network intrusion and options for detection and remediation remain suspect. IBM and Ponemon's 2018 Cost of a Data Breach[1] study shows that data breaches are becoming bigger and costlier year after year, and McAfee's 2018 Mobile Threat Report declared 2018[2] to be the riskiest year yet. Are organizations prepared for acceleration of these cyber-security risk factors?

Today, typical-best practice for mobile security includes a reliance on Enterprise Mobility Management (EMM) systems primarily designed for mobile device procurement, deployment and general management. These tools can be helpful for devices operationally, but EMM was never built with security top of mind. The main mobile security features in EMM software are the remote wiping function and some identity and asset management functions. Additionally, EMM systems add antivirus solutions that do a good job of "watching" for malicious software code. However, AV systems need constant daily updates (some every hour) to their embedded virus definition files that identify threats. A recent InfoSecurity Article[3] reports that there are at least 360,000 new malicious virus files introduced to the world's computers every day. Maintaining AV in today's cyber landscape is a constant game of hit and miss for InfoSec professionals.

It's also important to note, in certain industries, if a device is compromised to the point where a remote wipe is warranted, it is already too late. For information security, compliance and audit purposes, IT managers need to selectively collect and archive individual device log data for every application launched, every file stored, every email, every website accessed, and every location tracked by GPS. These are standard procedures in enterprise network security but uniquely difficult when it comes to mobile devices because they are

1 *https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf*
2 *https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2018.pdf*
3 *https://www.infosecurity-magazine.com/news/360k-new-malware-samples-every-day/s*

at the far reaches of network perimeters and their log data is not native to InfoSec systems. They were never built to offer this kind of visibility to InfoSec managers. Furthermore, this visibility generally isn't offered with event log correlation capabilities in EMM platforms because they are not Security Information and Event Management or SIEM systems.

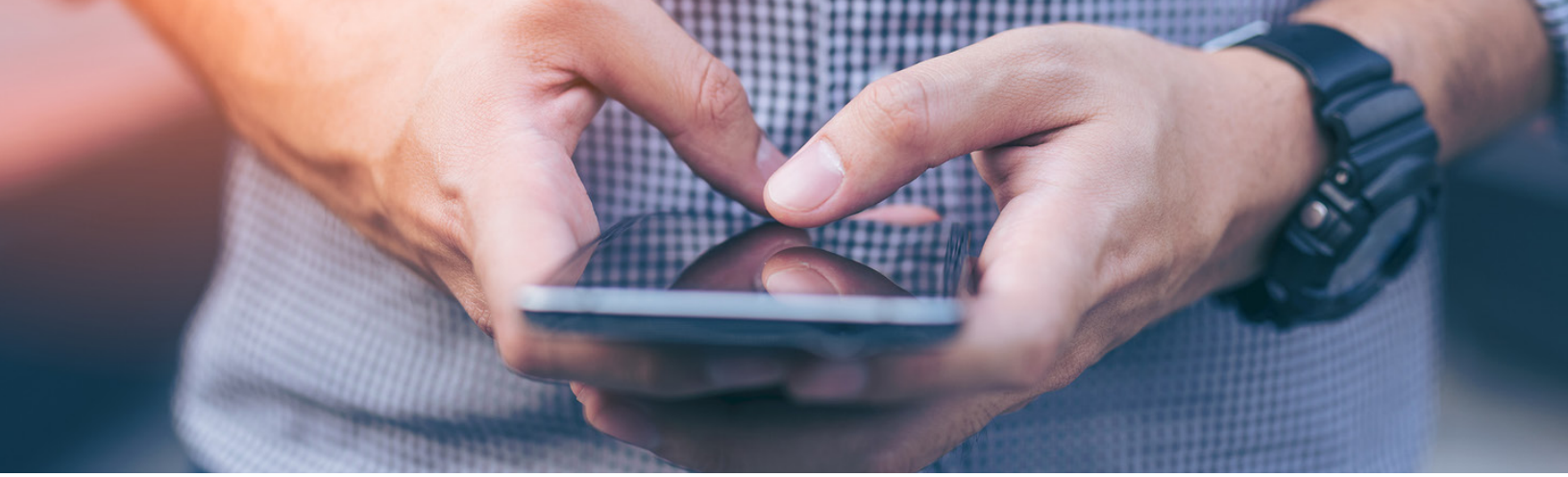
Education Is Just the Start

To make sure employees have a fighting chance when it comes to mobile security, you need to make sure that they are educated. A recent Ponemon/Opus[4] Research survey, "What CISOs Worry About in 2018" revealed that employee cyber incompetence and negligence are high on CISOs' list of worries. When asked which threats they worry about most, 70 percent of CISOs said lack of competence of in-house staff and 54 percent stated inability to reduce employee negligence.

The ubiquitous mobile device has become an extension of our persona, an extended computerized appendage in our hands nearly every waking minute of most our days. A false sense of security exists with most when it comes to their mobile devices because their devices are viewed personal assistant and fun devices first, mini business computers second. Fact is, most people simply don't know what best practice security is for their PII and sensitive mobile data at risk – both personal and corporate. One study of a Philippine University[5] found that most faculty and students saved sensitive data like ATM pins, passwords, images and video on their devices without any encryption methods. Fifty percent of the study's participants did not know about the security features of their phone. While Higher Education is not generally known for its high levels of IT maturity, the results of the study are very indicative of employees' approach to mobile device use (and it's not security!) where social media, chat and gaming rule the day. This false sense of security inherent in users of mobile technology is cause for great concern for enterprise organizations needing to protect corporate IP and identity data to compliance standards. The initial battles for securing your organization's data and IP should be fought with education during new-hire onboarding and through every continuing ed opportunity.

Another problem that affects enterprise data and IP is that most users simply forego security precautions in Bring Your Own Device (BYOD) environments when it hampers their productivity. Because EMM solutions were never intended to secure the network – this is the SIEM's job – the answer to outer-perimeter security when the mobile device came along was to close access to all enterprise systems outside the network perimeter, leaving users without the ability to use data and apps on the device to do their

4 *https://www.opus.com/resource/2018-ciso-survey-ponemon-institute/*
5 *https://www.researchgate.net/publication/328734205_Mobile_Security_Practices_of_Faculty_and_Students_in_a_Philippine_State_University*



jobs. Employee productivity via mobile has become hampered by these practices, and rather than be inefficient away from their offices, employees have found other outside-of-policy mobile applications and tools to help them get their jobs done. The result is a higher risk to network intrusion because many of these mobile apps are accessing company networks without network security managers even knowing the apps are on the mobile devices. When you consider that mobile app developers aren't security experts – many are designers using app development platforms – mobile has become ripe for cyber disaster.

Many employers have adopted Corporate Owned Personal Device (COPD) policies but millennial and Gen Z employees prefer their personal devices and don't want to carry two phones around. In this scenario, COPD could end up costing young talented employees who choose to work with a more progressive company that offers BYOD. But as mentioned previously, the BYOD-managed-by-EMM model delivers a hampered user experience because of the locked-down mobile security policy. There is however, another option to consider.

BYOD 2.0 Enabled by Containerization

Mobile security "containerization" is an attractive alternative to offering employees separate environments on the same device for both personal and work data use. This method of mobile security uses a virtual container on the device to segment personal apps from corporate data and apps fortified with encryption and authentication. With an encrypted container, enterprise apps and data are separated from personal apps both on the device and across any data transmitted to and from the enterprise. Because of the separation of data and apps within the container, AV is not needed. A virus could attack the personal partition of the phone, but with the container separating the data and apps communicating with the data center, the environment remains safe within the container.

This ability to manage data and apps within mobile environments creates work processes far outside the network perimeter similar to a desktop experience in the office without the constraints of multiple VPN connections. In these scenarios, a CMO can approve an ad in his/her organization's project management system from their mobile device in another country if needed. Similarly, a head of HR can approve the onboarding of an urgent new hire across the organization's ERP system while on vacation, all within the container. This new way of replicating an in-office experience in a secure, segmented environment on a mobile device is what SyncDog defines as BYOD 2.0, and the containerized solution SyncDog delivers is Secure. Systems™.

Industry analysts agree that containerization is an excellent approach to mobile data security, but the drawback to this approach is the flexibility EMMs employ to handle different application frameworks and APIs. Former president Obama once famously

asked[6] his security team to produce a secure mobile phone for him to use once he made his transition to the White House, so he could stay in touch with friends and loved ones. What his team came up with was a military-grade phone without a microphone, camera, or location tracker that could not make or receive calls or texts. While this was the most secure option, he still couldn't talk to his loved ones nor use the device in any government-facing capacity. The president wanted security, but he also wanted to do business as usual and still be able to use his device for communicating with friends and family. The containerized workspace solves many of these challenges. SyncDog's mobile security container, Secure.Systems™, delivers NIST-approved security and a host of functionality across an expansive mobile app portfolio.

Secure.Systems™ removes limitations from overly-restrictive mobile security policies and allows for unimpeded and totally secure collaboration between mobile employees and their enterprise. Secure.Systems™ is protected through a FIPS 140-2 compliant, AES 256-bit encrypted app container.

Inside the secure container, you can allow employees to have access to most of the enterprise apps available to them as if they were on their laptops. Communication, file management, internet/intranet connection, and location-based services are all available within the Secure.Systems™ workspace. You don't have to worry if you miss a malware definition update on the phone's AV software because of the separation of data and apps on the phone within the container; AV software would not be needed.

With Secure.Systems™, you get a defense-grade, containerized workspace that serves as a complementary layer of security to your existing EMM investment. Your mobile app workspace is fully integrated while your network perimeter remains secure. Secure.Systems™ is currently integrated with Microsoft Intune, MobileIron, and other EMM systems. For more information on the Secure.Systems™ container from SyncDog, please visit www.syncdog.com.

Relying on Virus Definition Updates is High Risk: BYOD 2.0 is the Answer

The mobile computing footprint has exploded. In some parts of the world it has completely surpassed desktop use. Sixty-six percent of the world's population now uses a mobile device.[7] In the developing world, mobile use is staggering at 98.7 percent.[8] We are a mobile society with millennials and Gen Z workers comprising the largest population segment (ages 15-64) on earth. At 63 percent,[9] this is now the largest segment of the global workforce. They are perpetually online; consuming massive amounts of data and applications and they are always connected. AND, the have devices that are accessing your network with applications that you don't even know about, even as you read this paper.

The sheer number of mobile devices and accompanying network activity from these devices – 24/7 and 365 days a year – obliterates your network perimeter. Arguably, mobile access points have eliminated the concept of network perimeter altogether.

Securing all access points and applications across all devices is unattainable. One simple and highly

6 *https://www.politico.com/story/2018/05/21/trump-phone-security-risk-hackers-601903*
7 *https://www.slideshare.net/wearesocialsg/digital-in-2017-global-overview*
8 *https://www.theregister.co.uk/2017/08/03/itu_facts_and_figures_2017/*
9 *https://countrymeters.info/en/World#age_structure*

effective approach is encrypted data separation. Data separation on the device is the easiest, most economical (and perhaps only) way to protect your network from this mobile onslaught. SyncDog's innovative way to manage the mobility of this younger volitively digital workforce (BYOD 2.0) is relatively simple in concept. Antivirus is difficult. Relying on a virus definition update in your malware detection tool that may or may not have the latest virus or ransomware signature files should be keeping CISOs up at night.

> "Antivirus systems are a bandage, a finger in a dam with other holes you can't get to because there is no virus definition for the next malware threat to open the floodgates."

Another way that makes containerization a better option is that you can give employees a secure app environment in the container with all the business tools they need to do their job. In this application platform environment, employees can select and install business apps and productivity tools approved by your organization much like they would add games from an Apple or Android mobile store.

As with any other aspect of business, companies must either adapt or become irrelevant. Businesses that embrace BYOD 2.0 as a better alternative to the EMM/antivirus/locked-down-app way of providing mobile security can provide employees with additional and better tools to get the job done. These BYOD 2.0 businesses will adapt and conquer because they can sign POs faster, approve new hires faster, and provide more collaborative communication and business workflows better than their competitors.

But the process comes with the caveat of maintaining data protection. Data protection laws such as the GDPR and now U.S. states' legislation leave little room for mistakes with corporate, government and now personally identifiable information (PII). Antivirus systems are a bandage, a finger in a dam with other holes you can't get to because there is no virus definition for the next malware threat to open the floodgates. Containerization is the logical solution to simplify data protection at the point of attack because it is simple data separation with a blanket of encryption for data on the device and in transit, regardless of location of the user.

SyncDog's Secure.Systems™ containerized workspace is an exceptional choice when addressing mobile security across a mobile generation that commands high functionality to get the job done. The solution is easy to deploy and maintain, has a low cost of ownership, and can be used as standalone solution or in conjunction with any existing EMM system. To see a full list of applications in the containerized workspace or to learn about existing integrations, download our data sheet here, or visit www.syncdog.com to learn more

SECURE.SYSTEMS

PROTECTED BY SYNCDOG

11921 Freedom Drive, Suite 1120
Reston, VA 20190
Call: (703) 430-6040 • Fax: (703) 997-8667
www.syncdog.com