BYOD Challenges Traditional Security

Everyone seems to have a smartphone, iPad, notepad, etc. Proliferation of devices over the last 5 years has given way to people wanting a "one-stop-shop" for all their communication needs—personal as well as work related.

Enabling users to work anytime anywhere can be a great boost to productivity and employee satisfaction. Flexible IT policies that enable use of personal devices for business use can make for happy workers, and happy workers tend to work harder—plus companies can be more competitive and yield higher recruiting rates. A few quick facts:

- **83% more satisfied with their job** with access to flexible IT policies (Deloitte)
- **51% of younger employees would circumvent any policy** that restricts use of personal devices (Fortinet)
- **50%+ companies plan BYOD** exclusively by 2017 (Gartner)

BYOD Improves Productivity, Employee Retention and Reduces Workloads

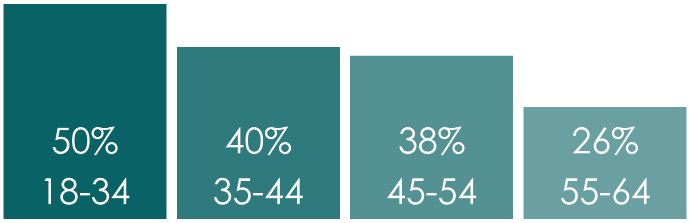
- 57 minutes daily productivity increase with a BYOD program (annual gain of 1.6 million hours!) (Intel)
- 240 more hours per year productivity increase for employees who use their mobile devices for work (Cap Gemini Consulting)
- **Employee retention**—happy employees stay with a company longer. Global consulting firm Deloitte found that 83% of employees were more satisfied with their job when IT policies enabled them access to BYOD and telecommuting
- **Low to no training costs**—Employees train themselves
- **Less work for IT**—Employees handle their own device upgrades which lessens burden on IT and saves money

BYOD Challenges Traditional Security

The dark side of BYOD represents one of the biggest shifts ever seen in terms of security. BYOD can impact traditional security models of protecting the perimeter of the organization by defining the perimeter in terms of physical location and asset ownership (company-owned vs employee-owned in the case of BYOD).

BYOD personal devices used for work-related activities can contain corporate credentials or log-in information—easy access for cybercriminals into the corporate network. In addition, these devices also may contain apps or links that make them more vulnerable to hackers.

Percentage of work device usage by age demographic



Source: Webroot Mobile Security Report 7/14

Two types of security risks with BYOD include:

- **Malicious apps (malware):** the number of apps and source of apps on an employee's personal device increase the likelihood that some may contain malicious code or security holes that hackers may exploit
- **App vulnerabilities:** company-owned apps to access corporate data may be compromised once installed on an employee-owned device

Everything comes at a cost—and with BYOD, that cost is paid by the business' security. It only takes one compromised device to put all corporate data and resources at risk. How likely is it for these devices to be compromised? Unfortunately, it's a lot more likely than we would probably care to admit. Consider:

- **51% of smartphones users connect to unsecured wireless networks**, often exploited to perpetrate man-in-the-middle (MitM) attacks and distribute malware – Cisco

- More than **10 million malicious Android applications** have been identified - Kaspersky
- **60% of mobile malware** includes elements of **large or small botnets** - Kaspersky
- Apple, which is often considered a "secure" operating system, revealed **security flaws** in their iPhones' and iPad's iOS that could have allowed **MitM attacks and malware** to be downloaded

When using smartphones and tablets, users often bypass traditional security checks and perimeter defenses, "walking" their compromised devices straight into the corporate environment to access their emails, corporate applications, files, etc.

Once in the environment, sophisticated attackers simply sit and wait for their moment to use the access they now have to target high value corporate information and resources. It is important that organizations are prepared, adding a layer of security that can identify and stop these attacks before they can do any damage. It requires solutions that can unobtrusively guard internal resources from attacks, regardless of when, where or how they enter the network.

Uncover Attacks that Walk in the Door

With the BOTsink™ Solution, you can immediately uncover attacks brought into your network, typically unwittingly by users who often bypass existing security measures—you quickly and accurately identify BOTs and APTs on your network that may have been introduced by infected:

- Employee-owned devices—BYOD
- Mobile workers accessing resources remotely, outside the firewall
- 3rd party vendors and suppliers

Attivo's BOTsink Solution has been purpose-built to provide enterprises a set-and-forget, **self-contained breach detection solution.** Unlike traditional in-line solutions looking for attacks using signatures or attack patterns and known C&C addresses to identify suspicious activity, Attivo's BOTsink Solution sends and attracts the attackers to it. The BOTsink Solution can send targeted BOTs and APTs to its engagement servers and lures scanning attacks to engage and then springs into action, delivering accurate, definitive information on the BOTs and APTs, so you can eliminate the threat.

With Attivo you can gain visibility into the effectiveness of your security infrastructure and reduce detection time of BOTs and APTs, so they can be shut them down before they can do any damage.

Attivo's Unique Virtual HoneyNet Solution

The Attivo BOTsink Solution is ideal for defending against BOTs and APTs brought into your network via a host of BYOD devices. With an Attivo BOTsink interleaved throughout your network, you will be able to:

- **Reduces Attack Detection Time**—providing accurate, actionable alerts that quickly and accurately identify infected clients, including sleeper and time-triggered agents, to enable remediation of the full extent of the attack before it can do any damage
- **Capture Actionable Information**—identifies the infected client, it prevents any ongoing communications outside the appliance to stop the attack's propagation
- **Destroy the APTs and BOTs**—prevents whatever comes in from ever getting out—stops the attack and destroys the BOT and APT once data is collected
- **Guards your network 24x7x365**—self-contained solution constantly monitors activity and rebuilds itself to ensure optimal performance

For more information about Attivo Networks BOTsink Solutions or to schedule a demonstration, contact sales@attivonetworks.com