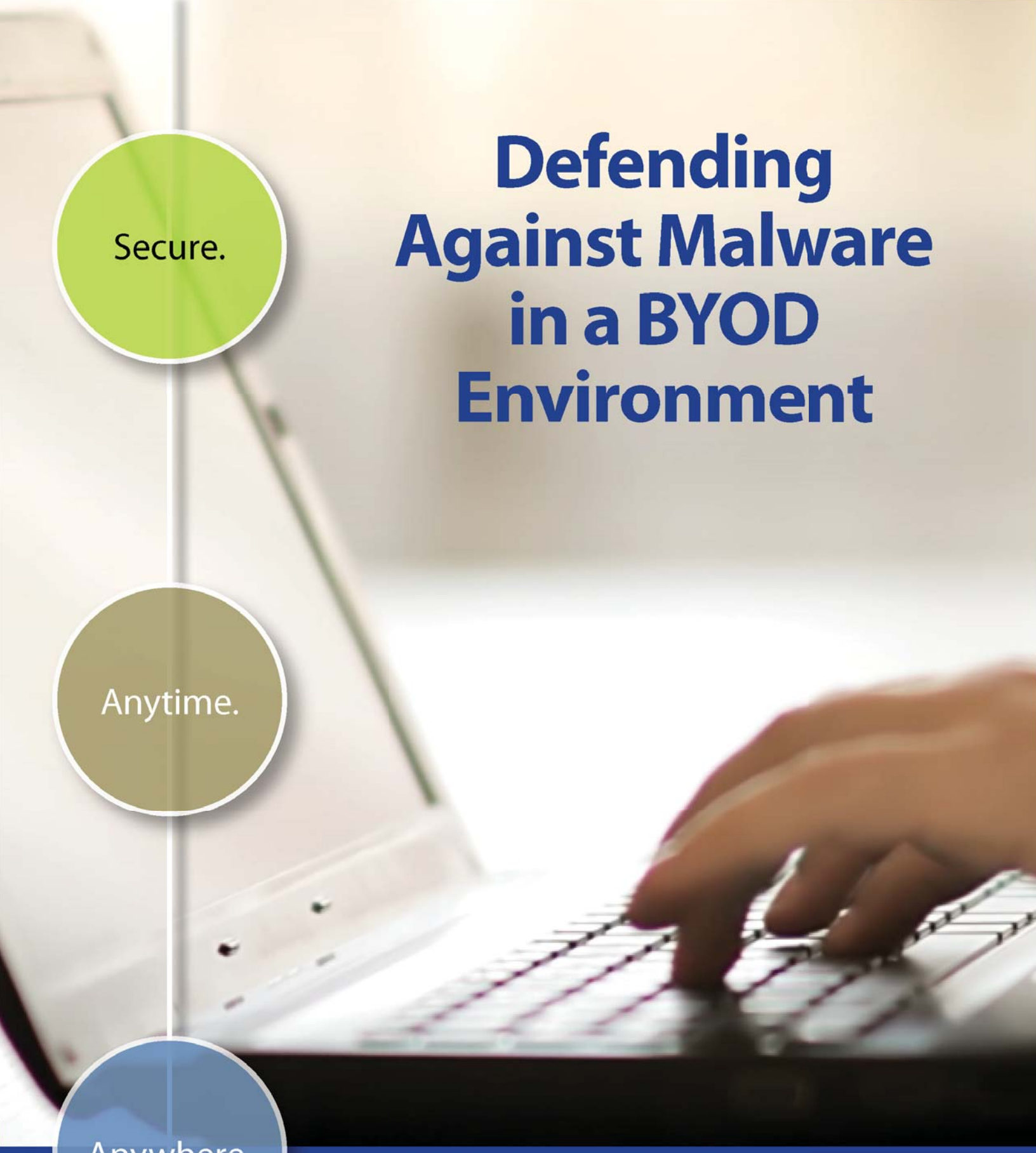


Defending Against Malware in a BYOD Environment

KANGURU™
Secure. Anytime. Anywhere.

Defending Against Malware in a BYOD Environment

Introduction

Bring Your Own Device, or BYOD is taking the IT world by storm. This policy of allowing employees to use their own computing device, rather than a device issued by the IT Department, is changing the way organizations think about IT asset management and security. BYOD is also an acknowledgement that employees are using these devices already, and it is better to adapt than resist.

While BYOD has many advantages, including reduced overhead costs, it can also lead to an increased vulnerability to malware and other security threats. The IT Department once had control over all company devices and ensured that each one was secured through anti-virus software, firewalls and restricted OS access. These days, employees could be accessing sensitive information from a laptop or home computer that is outside of the company's control. When implementing a BYOD policy, it is important to consider these threats and take steps to reduce the risk of data breach.

Security Threats

Browser Trojans

This type of malware infects a web browser and then modifies web pages or online transactions. The so-called Man-in-the-Browser (MITB) malware is similar to the classic Man-in-the-Middle attack, in that a 3rd party inserts itself between two communication points. The spyware might intercept communication between a computer user and his or her bank website, for example. One well known browser Trojan is the "Zeus" virus, which has been used to steal bank passwords, credit card numbers, and other personal data. Though Zeus originally spread via spam email, the virus is now infecting browsers through Facebook and other social media sites. [1]

Phishing

Phishing is an attempt to trick users into revealing sensitive data. The criminals pose as a legitimate business and take advantage of a trusted relationship that already exists. This is often done by sending fake emails that appear to have come from the user's financial institution or social media site. Sometimes a user is prompted to enter passwords or account numbers. Other times the phishing attempt will convince the victim to click on a link to malware. Studies have estimated an annual loss of $3 Billion caused by phishing attacks. [2]

Keyloggers

This type of malware installs itself on a computer and then records all of the keystrokes that are typed by the user. The victim is often completely unaware that the keylogger is installed and running in the background. With this spyware in place, it becomes easy for a criminal to record passwords, financial data and other sensitive information. A recent report shows that 75% of all malware attacks in the past year included the use of a spyware or keylogger application. [3]

Loss or Theft

With so many portable devices being introduced in the work place, it is inevitable that many devices will be lost or stolen. An unprotected laptop, USB device or smartphone could contain a large amount of data that is now exposed to unauthorized access. A data breach that reveals customer or employee information can result in damaged reputation or even lawsuits. Organizations that suffer a data breach through portable devices are often forced to pay for credit-monitoring for all those who are affected.

Kanguru Defender DualTrust™

The security concerns above should be taken seriously, but they should not prevent an organization from implementing BYOD policies. With the right technology and training in place, security threats can be mitigated. The Kanguru Defender DualTrust is one easy-to-use tool for implementing BYOD securely.

Defender DualTrust is a combination of an encrypted USB flash drive, an isolated virtual machine and a secure web browser. The Defender DualTrust can be plugged into any Windows computer to create a Secure Virtual Workspace™ for accessing online resources. After the user enters the correct password, the device launches a virtual machine that is isolated from the host operating system and runs a separate, hardened virtual OS from the encrypted partition of the device. Running inside that OS is a protected Chrome browser. This enables employees to use their own laptop, home computer or other PC without being exposed to malware in host OS.

Figure 1: Security Architecture

Simple Protection Against Malware

The Kanguru Defender DualTrust offers protection against the most common forms of data loss and identity theft:

BROWSER TROJAN	The Defender DualTrust protects against Man-In-The-Browser attacks by launching a secure web browser that is isolated from any malware in the host operating system. The secure virtual machine generates a new, clean session each time the device is plugged in.
PHISHING	Using Defender DualTrust is a great defense against malicious web links and fake websites. Instead of clicking on unsecure links, users can open a protected browsing session and type the correct website address. This prevents malware from redirecting web traffic away from legitimate sites.
KEYLOGGER	Keyloggers, spyware and other malicious software code that is installed on a computer can be blocked by using the Defender DualTrust. The device generates a virtual machine and hardened OS that is isolated from the host OS. Malware on the host machine will be unable to intercept keystrokes or other data that is inside the protected session.
LOSS OR THEFT	Defender DualTrust is hardware encrypted with military-grade AES-256 Encryption. Sensitive data can be securely stored on the device without the risk of unauthorized access. Data encryption is automatic and transparent to the user. If the device is lost or stolen, no one can access the drive without the password. Additional security is available through the Kanguru Remote Management Console software, which can track Defender DualTrust devices anywhere they connect. If a device is lost or stolen, the IT administrator can remotely wipe or disable the drive.

Best Practices

These precautions are recommended when developing a BYOD policy:

1. Provide employees with tools to secure their computer before accessing corporate resources.
2. Ensure that browsers and applications run inside secure containers, such as the Defender DualTrust Secure Virtual Workspace, in order to prevent spyware from recording data.
3. To prevent phishing attempts, type URL's directly into a secure browser rather than clicking untrusted links.
4. Thwart Trojan malware by starting with a clean browser installation every time. Defender DualTrust creates a fresh virtual machine and browser upon each login.

Conclusion

Security threats should not prevent organizations from implementing BYOD policies if they make sense from a business and technology standpoint. While there are legitimate security concerns that are not to be taken lightly, these risks can be reduced by protecting the way employees access company resources. The Kanguru Defender DualTrust is an easy way to implement BYOD safely. With this protective shield, users can use personal computers and laptops without exposing the organization to data loss.

References:

[1] New York Times, Bits Blog,
http://bits.blogs.nytimes.com/2013/06/03/malware-that-drains-your-bank-account-thriving-on-facebook/

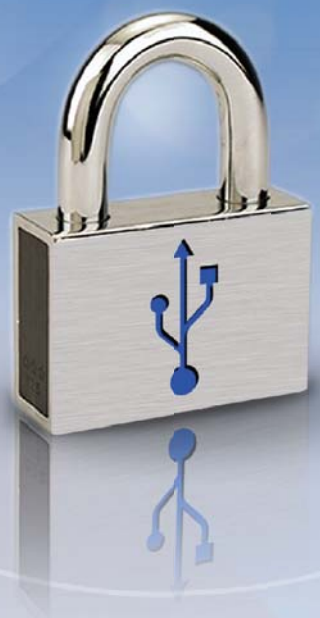
[2] Gartner Survey, http://www.gartner.com/newsroom/id/565125

[3] Verizon 2013 Data Breach Investigation Report, Page 30, http://www.verizonenterprise.com/DBIR/2013/

Secure.

Anytime.

Anywhere.



KANGURU™

1360 Main Street

Millis Massachusetts 02054

888-KANGURU

508.376.4245

sales@kanguru.com

www.kanguru.com