EVIDEN

Digital Security Magazine - 11th edition
July 2023

BYOD and the power of protection

By Dwayne Natwick

Bring your own device (BYOD) has grown exponentially over the past five years.

Today, everyone has a smart phone that can access the web and email in the palm of their hands. The expansion of work from home since 2020 has provided an opportunity for companies to save money on equipment by allowing their users to access their own personal devices. Cloud applications allow access to personal and company resources from anywhere at any time.

But with this increase in convenience, there is also an increase in vulnerability.

Shedding light on BYOD

BYOD refers to any device that is provided by the user and may be used to access personal and business information. While this provides users with flexibility (they can choose their preferred equipment), it saves businesses the need for a capital expense budget for devices. However, this may also create risks and vulnerabilities to the business.

These include viruses and malware, exposure of sensitive data, insecure network connections, and lost or stolen equipment. In this article, you will learn techniques to secure and protect these devices from falling victim to these risks and vulnerabilities.

Veering away from viruses and malware

Yes, computer viruses and malware are still out there and causing issues with devices.Infected devices knock a user offline and can cause a drop in business efficiency andeffectiveness. Since these devices are personally owned, the business may not have theauthority to enforce critical security updates. Unfortunately, infected systems that areconnected to a company's network can infect other devices and cause even moredevices to go down. In addition, malware can be used to deliver ransomware onto yourdevices and into your systems. How can we avoid these infections?

Even though these devices are personally owned, the business has a responsibility toprotect their data. This includes any personal identifiable information (PII) and anyintellectual property (IP) that is held within the business. Therefore, the business shouldhave a policy wherein any personal devices that are accessing company information musthave endpoint protection in place. Endpoint protection will reduce the attack surface ofthe device. Many endpoint protection software solutions also have anti-virus and anti-malware built in.

To enforce endpoint protection and verify that devices are properly patched, mobiledevice management (MDM) is highly recommended. MDM will manage a device and pushout policies to maintain proper levels of compliance for the business. Devices that are notcompliant with these policies may be blocked from accessing business applications untilthey have been properly patched and updated. Users that want to utilize their personaldevices are hesitant to install MDM solutions because they feel that it is too invasive. Inhighly regulated businesses, this may be the only option for a BYOD policy.

Securing sensitive data protection

Another risk and vulnerability when utilizing BYOD is potential sensitive data loss. Sensitive data includes PII, IP, and personal health information (PHI). Exposure and loss of this information can cause identity theft and damage to the business' reputation. To protect against this risk, you should protect against users saving business data locally, sharing through email, or utilizing cloud applications that are not approved.

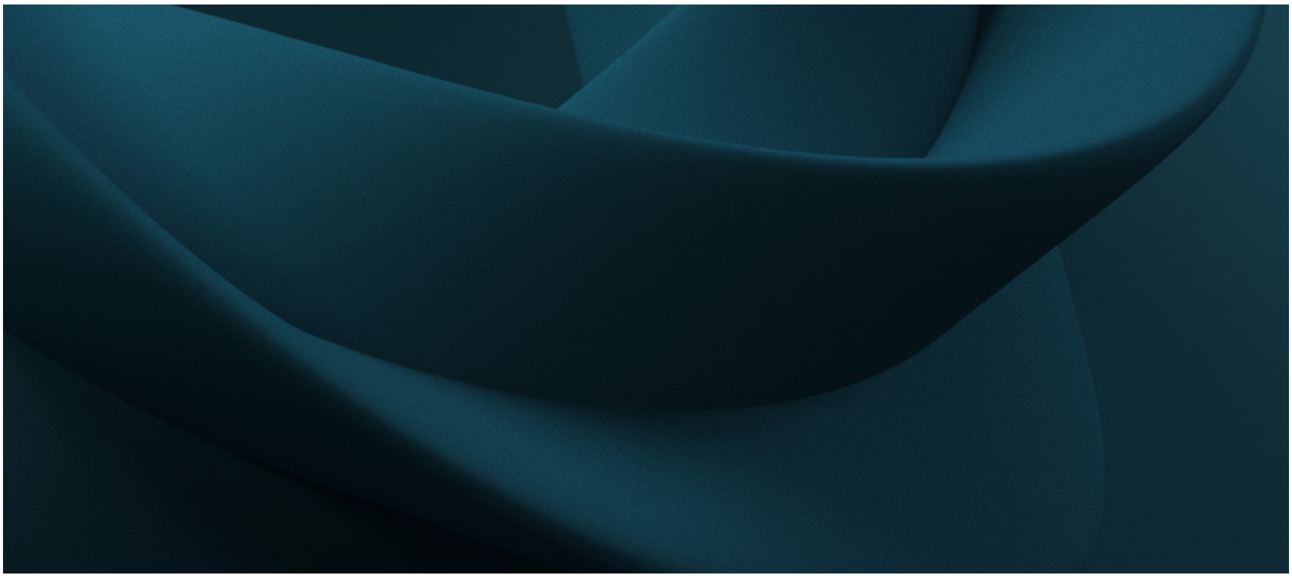
Solutions that can protect against this are data loss prevention solutions (DLP) and cloud access security broker (CASB) solutions. DLPs can block oversharing of sensitive information, which may include the ability to copy/paste a cloud storage sharing link on a personal device. CASB can block the printing or downloading of information, and block access to cloud applications that are not approved by the business for use and sharing of data.

MDM solutions can also be used to protect against data loss and enforce policies for sharing data. Alternatively, mobile application management (MAM) is a less invasive option to users than MDM as it is better suited to those businesses which may want to provide more flexibility to users. MAM solutions allow for those applications accessing business information to be managed by the policies, thereby protecting business data from being used in personal applications, files, and browsers.

Securing network connections

BYOD are generally portable devices and can access the Internet from anywhere. But how secure is the Internet that the device is connecting to? Before applications were accessible directly through the Internet, businesses would only allow remote access through a secure VPN connection. Though VPNs are still used, they are not as widely enforced as they used to be. This requires users to take care and follow due diligence in the networks that they are using to access company information. They should not be accessing sensitive information over an unknown or public network, such as unprotected Wi-Fi in a coffee shop.

However, users do not always understand their responsibility and the need for security, so the business should have network policies in place. These policies may enforce a secure VPN connection when accessing a business application through a public Internet connection. To enforce these policies, MAM can be used. Additionally, they may use condition-based policies that manage the authentication and authorization of access to business applications.



Recovering lost or stolen equipment

The final risk with BYOD is a risk that you can have with any portable device — loss or theft. Allowing users to access business applications on their personal devices poses a risk to sensitive data being exposed, especially if that device is lost or stolen. How do we prevent such a device from accessing data that may damage the business, its people, or its customers?

The easiest way to do this is to have a policy to lock these devices with PIN and biometrics. The device can then not be accessed by those that recover the device. MDM or MAM are more secure manners to protect these devices. Now, these solutions maintain a connection to the devices when they are on the Internet, allowing the business to erase and disconnect the business data from the device. Having MDM or MAM installed may also trigger location services to find out where the device is for recovery.

Maximizing BYOD for business benefits

MDM or MAM solutions are one of the better ways to protect and secure business data and applications on BYOD. Another option that is even more secure is to use a virtual desktop for users to access any personal devices. Virtual desktops give users a cloud version of Windows or Linux operating systems with contained access to applications in a familiar interface. A virtual desktop deployment can be complex and would warrant a full article on its own.

BYOD is a flexible solution that can aid in decreasing capital expenses for a business. However, as earlier mentioned, this introduces a level of risk and vulnerability that needs to be planned for and addressed. This includes having clear and defined policies for users regarding what they can access on these devices, what they can share, and what management and security tools will be installed by the business to protect business information on these devices. If you have these policies in place and provide users with the proper training,

BYOD can be a successful tool in the business world!

Connect with us

eviden.com