MODEL TECHNOLOGY SOLUTIONS

Cybersecurity Simplified: Protect Data on Personal Devices

Bring your own device (BYOD) refers to a policy of permitting employees to use personally-owned devices (laptops, tablets, and smartphones) to access company information and applications. BYOD continues to grow in popularity among businesses as a means to increase mobile and work from anywhere productivity choices for employees or reduce hardware expenditures.

However, endpoint security can be a concern when it comes to BYOD. With an influx of personal devices in the workplace, the possibility of viruses, hacks, and data leaks is elevated. Every device that accesses company information represents an additional endpoint that hackers can attempt to breach.

There are several reasons to offer a BYOD policy:

- **Increased worker satisfaction.** Employees can use the devices they prefer and enjoy greater productivity because they are using familiar tools.
- **Less IT burden.** Having employees take care of their own device's maintenance means less involvement and work from the information technology's (IT) department.
- **Saving money.** Employees pay for their own devices and the maintenance that goes along with them.
- **Increased employee engagement.** Employees can get work done without having to physically be at the office. This gives them greater flexibility to manage their schedules and stay on top of their work.

What steps can you take to reduce the risks of BYOD?

Traditional mobile endpoint threat management solutions involve controlling all aspects of a mobile device, which many companies are reluctant to do for devices that their employees own. A better approach is a system that allows work-related applications to be securely managed while leaving personal apps and data alone.

Microsoft 365 Business Premium protects company data on your staff's personal devices.

Microsoft 365 Business Premium (formerly Microsoft 365 Business) supports Mobile Application Management, via Intune which helps you to securely manage apps and data on iOS, Android and Windows devices.

You can control which apps are allowed to access company data. You can require users to access work data from the Office mobile apps and configure policies that keep the data protected (such as encrypting it, protecting it with a PIN, and so on).

You can also help prevent users from moving data to an unsecured app. You can set policies to prevent a user from copying text from their company email and pasting it into an unsecure place, such as their email or the Notes app on their phone. You can block a user from saving a spreadsheet of customer data to personal cloud storage (like Dropbox, for instance).

You can also delete company data from a device if it is lost or stolen, or if an employee leaves the company. And you can do this without impacting personal data from the device. For example, if an employee leaves your company, you can remotely delete all company data from their phone, but their photos, personal contacts, and texts will be untouched.

Why should I use Microsoft 365 Business Premium to support my BYOD policy?

Microsoft Intune – the technology that powers the BYOD environments at many of the world's largest companies – is the technology used by Microsoft 365 Business Premium to support your BYOD policy. Employees can use familiar Office mobile apps instead of 3rd party apps required by other high-security solutions. These capabilities are included with your subscription – there are no additional 3rd party solutions to buy, install, or manage.

Healthcare

While health care environments have traditionally been limited to desktop computers in the office, this has begun to change. More professionals in the medical industry are using mobile and personal devices to stay connected when out of the office.

BYOD presents an endpoint security challenge in the health care industry, as devices containing Protected Health Information (PHI) need to comply with HIPPA\HITRUST regulations.

Microsoft provides several endpoint security solutions relevant to this problem. Microsoft Azure and Office 365 are the first hyperscale cloud services to be certified for the HITRUST CSF, and Intune is capable of enforcing policies on BYOD devices that safeguard PHI through encryption, passcodes, and wiping lost or stolen devices.

Though BYOD in health care has unique challenges, leveraging a powerful MDM solution like Intune can bridge the gap between using personal devices and protecting PHI.

TAKE ACTION, START TODAY

Find Your Cybersecurity Holes

Is the lack of a standardized BYOD policy opening your environment to threats? When you use our vCISO services, you'll identify key vulnerabilities (like BYOD) in your environment and create an expert strategy to close your holes. You'll save your team the time, budget, and consequences of focusing on the wrong solutions. Plus, you'll get access a full year of our expert guidance to help you improve.

Here's everything that's included for a year:

- Model's cybersecurity assessment
- 24x7 access to the Model vCISO portal
- Monthly vCSIO meetings with Model's expert cybersecurity director

START YOUR ASSESSMENT HERE