opentext™

Flash Point Paper

Data Privacy: Keys to Keeping Your Corporate Data Secure

With the expanding number of different devices, apps and operating systems that corporate workers use to get their jobs done, protecting corporate data grows harder and harder.

The fast pace of today's dynamic digital workspace means your people need to be able to access critical information from any location using any device at any time. It's difficult enough securing that sensitive data on the desktops and servers within your network boundaries, but the task becomes undaunting as your workforce uses their laptops and mobile devices to access that work data while roaming the wilds of Internet cafes, airports, hotel rooms, public transportation, and the comfort of their own homes.

The key to protecting that data begins with being able to secure and manage all your endpoints from a central management console. And from that console, you need the ability to execute security capabilities and enforce security policies for four critical endpoint use cases.

BYO Use Case

Given a choice, many users prefer to use their own mobile devices for work as well as personal use—assuming there's minimal impact on the way they use those personal devices and no impact on their personal information stored on their devices. But how do you allow users freedom, while making sure any corporate data they access on their personal devices remains secure? The answer is a mobile application management (MAM) solution that lets you balance your need to secure your corporate assets while minimizing the impacts those necessary controls have on your mobile users' productivity and experiences.

MAM solutions can enforce security controls at the application level in a way that creates a separation between the user's personal assets on the mobile device and the corporate assets on the device. One of the most effective methods that MAM solutions use to create the necessary separation is to use containerization. This creates a secure portion on the device's storage that is separate from the rest of the device's storage. Inside the secure container is where corporate applications execute and corporate data resides in encrypted form. With MAM containerization you can implement security controls and rules that govern access and usage of the device's corporate apps and data in a way that keeps you secure, while not interfering with the user's normal device usage.

Mobile Management Use Case

Despite the security benefits and user freedom that MAM solutions deliver in a BYO scenario,

Questions to Ask Yourself About Endpoint Data Privacy

- *How do you currently secure and manage your mobile applications for BYO?*
- *How do you protect your external storage devices?*
- *Do you have encryption policies in place for your endpoints?*
- *How do you currently protect and manage all of your endpoints?*

you might want or need the complete control that mobile management can give you over your users' mobile devices—whether company-owned or BYO. With mobile management, you implement security policies and controls that can affect the entire mobile device. This can include policies that let you enforce password restrictions, password complexity, encryption settings, screen locks, and device inactivity settings.

Other capabilities typically include device control policies that let you allow or restrict users from accessing certain device features, such as the camera, web browser usage, and voice assistants. With a mobile management, solution you can remotely lock the entire device if you suspect it's been lost or stolen. In such cases, you can even do a complete wipe of all data on the device to make sure your corporate data doesn't fall into the wrong hands. To streamline your management efforts and eliminate potential security governance gaps, it's a best practice to employ a mobile management solution that can be managed through the same web console used to secure and manage your organization's laptops, desktops, and servers.

Unauthorized Physical Access Use Case

Someone steps away from their office desktop just for a few minutes. Maybe they leave their laptop on a restaurant table while they use the restroom. Or perhaps a crook steals their computer from their backpack, car, or home. In any of these scenarios and many similar ones, there's a strong potential for an unauthorized person to gain physical access to the valuable corporate data stored on those endpoint devices. The best way to keep your sensitive corporate data secure in any of these situations is with full disk encryption, making your corporate information unreadable to unauthorized individuals.

Full disk encryption solutions vary by vendor, but some of the things to look for include support for both (FIPS) 140-2 Level 2 and Level 1 encryption modules, centralized key management, transparent encryption, background encryption, and decryption, and centralized pre-boot authentication override for when users forget their passwords. It's also nice to have the option to choose between pre-boot user authentication and normal windows authentication that gives the user a seamless experience.

Removable Media Use Case

Subset to the physical access use case are scenarios where someone tries to steal your data using thumb drives, CDs, DVDs, or any variety of external storage devices. How often do users step away from their computers for a moment without logging off? In those brief moments, it's easy for a thief to insert a thumb drive and start copying files and folders rich with your sensitive intellectual property or personal customer information. Protecting against that type of theft is easy if you have an endpoint security solution that lets you create and enforce policies that encrypt any data copied to removable storage. Without the encryption password, that data becomes worthless to would-be thieves.

You can strengthen your data protection even further with solutions and policies that completely block USB drives. So, if someone inserts a thumb drive and tries to copy files, they get an access denied error message. Such solutions often have whitelist options too, giving you granular controls over whether certain USB devices should be blocked or allowed. To complement these USB controls, you'll also want policies that control and govern your endpoint's ports, firewall protection, and wi-fi security based on whether users are in the office, at home, or using some unknown hotspot.

Everything You Need to Secure Your Endpoint Data

When it comes to securing corporate data on your organization's mobile devices, laptops, and desktops, OpenText™ delivers the full range of solutions you need. OpenText™ ZENworks Endpoint Security Management offers fine-grained, policy-based control over all your Windows desktops and laptops, including robust storage device controls, removable device data encryption, advanced firewall protection, wireless security, port controls, and application controls. OpenText™ ZENworks Full Disk Encryption makes it easy to automatically protect data stored on your laptops and desktops.

Connect with Us
OpenText CEO Mark Barrenechea's blog

When it comes to mobile management data protection, OpenText™ ZENworks Configuration Management provides advanced device security controls and policy management for iOS, Android, and other ActiveSync-enabled mobile devices, while allowing you to manage those devices from the same console that you use to manage your laptops, desktops, and servers. For your BYO needs, OpenText™ ZENworks Mobile Workspace gives you a best of breed MAM solution that empowers you to secure and control corporate data and applications on users' personal devices without impacting those users' personal use and files.

For more information on how OpenText solutions can work together to keep your corporate data safe and secure, visit: **www.microfocus.com/products/zenworks/endpoint-security-management/**

Learn more at
www.microfocus.com/opentext

opentext™