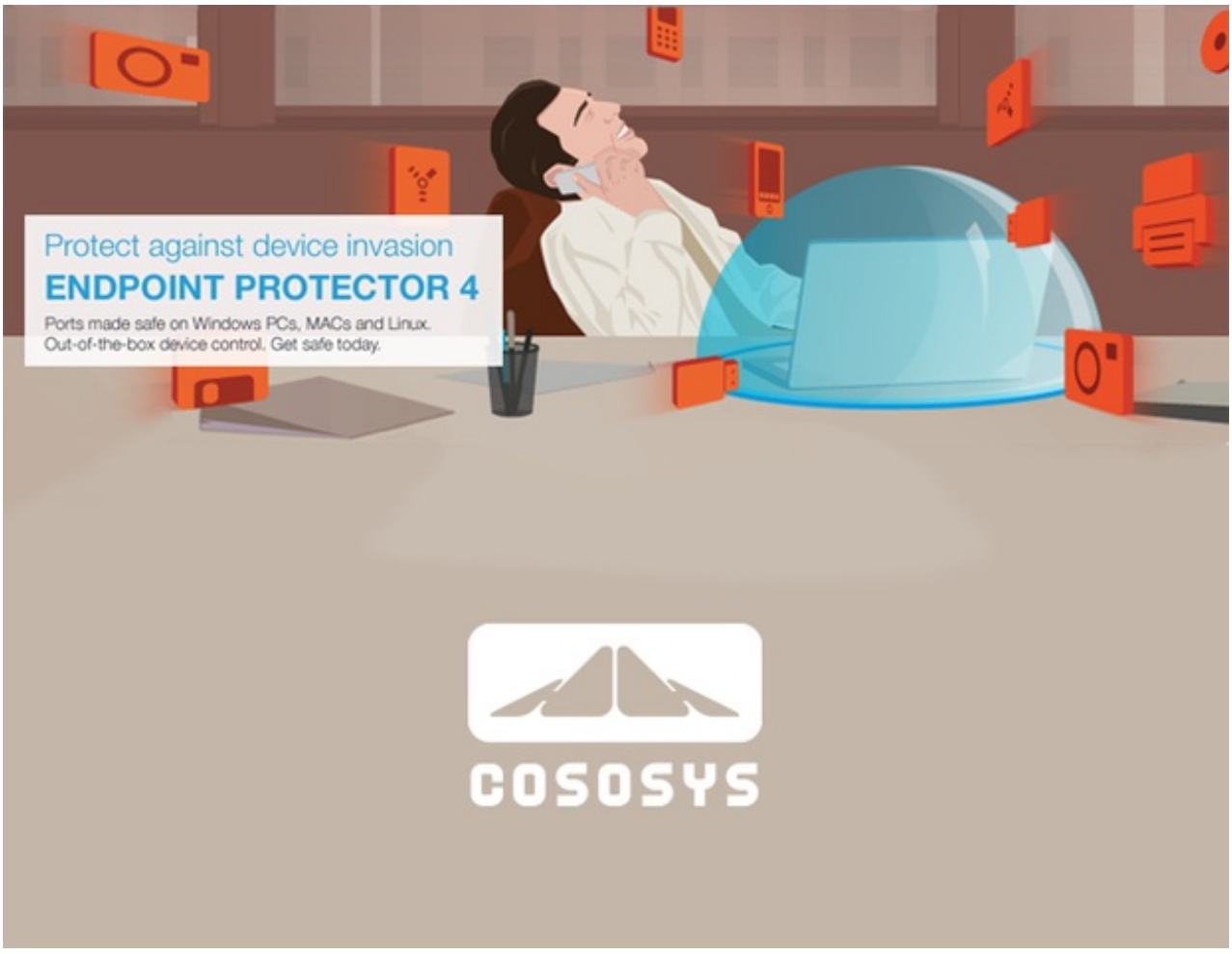
Enforce Mac storage device encryption with EndPoint Protector 4

By Erik Eckel April 7, 2014, 9:24 AM PST // erikeckel

Erik Eckel takes a look at Endpoint Protector 4, which helps Mac users and administrators force encryption use on USB flash drives and other portable storage media.

Mac



administrators have long struggled to enforce portable storage device encryption. Both Mac and Windows organizations -- where BYOD trends have introduced untold numbers of Macs to the network -- have fought to protect against the unauthorized release of sensitive, protected, or proprietary data. Yet, most users know how to connect an unauthorized thumb drive or external hard disk to an authorized and organization-administered computer. When those drives are subsequently lost or stolen, the corresponding data is at risk -- that is, unless the drive was properly encrypted, which is a task most users don't bother to learn or complete.

Enter CoSoSys Endpoint Protector 4. The application's EasyLock feature provides Mac users and administrators with the ability to force encryption use on USB flash drives and other portable storage media. The company also offers, for additional cost, a Content Aware Protection option that extends data protection enforcement to email clients and cloud services, such as Dropbox and Google Drive, and a Mobile Device Management (MDM) component for locking down iOS- and Android-powered tablets and smartphones.

After confirming security capability, ease of use and cost typically arise as the first elements most Mac businesses explore when contemplating security and encryption choices. Businesses will find EndPoint Protector capable on all fronts.

The platform and optional add-on components employ simple drag-and-drop- and copy-and-paste-like administrative actions. Organization data subsequently copied to portable media devices receives instant protection thanks to AES 256-bit encryption technology. Should unauthorized parties try to manipulate or otherwise tamper with the encrypted portable media, an additional security option enables deleting the disk's data.

As for cost, the software's priced reasonably for businesses needing to protect sensitive data. In an email exchange, the manufacturer's representatives confirmed pricing won't break the bank for a common small business. EndPoint Protector for Macs, combined with the EasyLock software that enforces encryption on portable storage devices, is $49.99 (USD) per license, the software is licensed per computer, and the license is a one-time fee. CoSoSys does maintain a handy cost calculator on its website, where businesses can explore myriad product, feature, and node combinations. Organizations with less than five users, meanwhile, can use the free Appetizer License software, although no support is included with that version.

A Web administration and administration console provide administrators with a centralized interface that can be used for encryption settings on numerous devices. Optional Content Aware Protection, which provides content inspection and logging capabilities, is available as an added service. Administrators can also leverage device-based policies and file-tracing features to further customize security settings and operation.

Why third-party encryption?

Some users may wonder why third-party encryption is required, due to Apple including the stout FileVault 2 encryption technology within OS X. It's a good question, but the reasons are many.

FileVault protects the Mac's internal disk. While some users may remember to exercise FileVault's capacity and encrypt external media, many will forget or never bother. Still others don't even use FileVault to encrypt their own Macs. EndPoint Protector with EasyLock and Content Aware Protection, when properly enabled, automatically enforces external media encryption, while adding a centralized Web administration interface, file tracing, policy configuration, logging capabilities, and even the ability to prohibit the copying of credit cards, social security numbers, and similar information.

The optional Content Aware Protection component extends administrators granular administrative control of organization data, thanks to content inspection technology that blocks data leaving via a wide mix of vulnerabilities, including clipboard, screen captures, and cloud-based services.

Do you use EndPoint Protector 4 in your organization? If not, how does your company protect sensitive company data when unencrypted and unauthorized thumb drives or external hard disks are connected to the network? Share your experience in the discussion thread below.