ITBUSINESSEDGE

Blogs: **Paul Mah**

Review of the CoSoSys Endpoint Protector Data Leakage Appliance

Posted by Paul Mah Oct 31, 2011 7:39:15 AM

The **CoSoSys Endpoint Protector** data leakage appliance is a dedicated appliance designed for the non-trivial task of device control and data loss prevention. Touted as an all-in-one device offering that works straight out of the box without the need for complicated server setup, the device secures endpoints with just a few clicks of the mouse.

As the Endpoint Protector comes with more abilities than I can cover here, I shall be highlighting its key features and my impressions of them below.

How It works

Setting up the Endpoint Protector is a simple matter of powering up the 1U device and configuring basic parameters such as its IP address. For pre-existing networks, the appliance supports the import of computers, groups and users via Active Directory. As you may expect, all system settings and security policies are configured from the Endpoint Protector's Web interface.

Once set up, the next step would be to deploy the Endpoint Protector client onto your Windows (64-bit supported) or Mac OS X workstations. This is done by downloading and executing a copy of the Endpoint Protector client software stored on the appliance from the target machine's Web browser. Once installed, the Endpoint Protector client cannot be disabled without the appropriate admin authorization.

Beyond restricting access to unauthorized external devices and storage locations, the Endpoint Protector client also helps to guard against intentional and inadvertent data leakage by communicating all file activities (and device changes) to the Endpoint Protector appliance in the background.

Device Management

The Endpoint Protector essentially monitors all devices from which data can be siphoned off. This includes USB flash drives, memory cards readers, storage devices such as floppy drives and CD/DVD readers and writers. In addition, the administrator can also limit access to devices such as biometric drives, Bluetooth, ExpressCard SSD devices, printers, as well as BlackBerry smartphones, iPhones, iPods and iPads.

The idea behind device management is simple: The act of identifying and preventing communication with external devices makes it possible to close off all avenues by which data can leak outside an organization without proper authorization.

Assigning Permissions

Access to specific devices can be defaulted to "allow" or "disallow" on a global, group or user basis. This allows for incredible flexibility: Managers can be defaulted to being able to use external storage devices. while line workers are only allowed to use the system, for example.

But how do permission changes work out for executives traveling out of town, and who may not have access to the Internet? This has already been thought out, and it is possible to perform an offline device authorization. Simply select the appropriate device to unlock, read out the code to the administrator over the phone, and key in the given unlock password. Presto! The selected device is now unlocked.

I was initially skeptical about the Endpoint Protector's ability to adequately detect the plethora of built-in and external devices on my laptop. However, the Endpoint Protector detected my Wi-Fi network, Bluetooth device, and even my virtual Wi-Fi adapter (Connectify) with ease. Another potential vector for data leakage, my laptop's built-in webcam, was also identified without a hitch. Other recognized devices were a portable USB hard disk drive, my connected iPhone and an internal DVD-RW drive.

File Tracing and File Shadowing

One of the most powerful features of the Endpoint Protector is its file-tracing and file-shadowing abilities. While device management is a powerful means of disabling the conduits by which data can be stolen or stored on unsecure devices, this does nothing to prevent authorized personnel from exploiting their legitimate access to surreptitiously copy out confidential customer databases prior to leaving the company.

To combat that, file shadowing creates an exact replica of all files in transmit from removable storage for audits. In addition, file tracing means that all data-related activities are also logged, including innocuous activities such as the renaming of files. Used together, file tracing and file shadowing effectively quashes attempts at misdirection by renaming files before

copying them out.

My Thoughts

The team behind the Endpoint Protector has done a stellar job in putting together a range of advanced capabilities into an easy-to-use appliance. If I must pinpoint a potential weakness of the Endpoint Protector, it would be how the multiple tiers of permission levels, plus the ability to perform group inheritance, mean that configuration mistakes could potentially be made. However, it can be rightfully argued that configuring any Windows Server comes with similar pitfalls.

In the final analysis, the onus is on the security administrator or IT manager to properly identify and craft the appropriate policies based on organizational needs, and implement them correctly on the Endpoint Protector.

Note that I tested the Endpoint Protector 2009, which has since been superseded by the newer Endpoint Protector 4, before the publication of this review. I was told that it comes with departmentalization and a cleaner interface, though the key capabilities outlined above remain the same. In the meantime, a virtual appliance version is available **here** as a trial for SMBs that want to determine its suitability.

More from our Network

The State of Our IT Security Vulnerabilities **CTO Edge**

Content Filtering Needs to Marry DLP **CTO Edge**

Why IT Security Projects Fail **CTO Edge**

Information Loss Prevention: The Key to Healthy Information Security **CTO Edge**

The Corporate Risks of Social Media **CTO Edge**

There are no comments on this post