Publishing and Printing company implements Data Loss Prevention, safeguarding copyright–protected content

PROFILE

Industry

Media

The Challenge

Prevent data loss and data theft of copyright-protected content and images

The Solution

Endpoint Protector 4

Why Endpoint Protector?

- Technically leading in monitoring Mac OS X
- Virtual Appliance is set up within a few minutes
- Intuitive user interface
- Offline Temporary Passwords for USB devices and computers

Stünings Medien uses Endpoint Protector 4 to prevent data loss and USB malware infection.

About Stünings Medien

Companies in the publishing and printing industry are often using Macs instead of Windows computers when it comes to producing their content. Reliability, comfort and design were the main reasons. Since users typically do not switch to Windows, Mac networks continue to grow and are especially popular in the media industry. That is the case for Stünings Medien GmbH, as well. Stünings' 110 employees are developing solutions in key areas like printing, publishing, internet and advertising, using 75 Apple computers.

Working with protected content

Stünings Medien is the biggest printing company in Krefeld (Germany), publishing journals, travel guides and reference books and developing websites and apps for smartphones and tablets. Employees' daily activities involve working with content that is copyright-protected by external authors or photographers. The challenge for Stünings Medien was finding a solution to avoiding unauthorized text or image being published and eliminate liability, financial risks as well as a bad reputation that such an incident would cause for the company.

>>

„With Endpoint Protector, we have the overview needed to evaluate the employees' activities. For example, it is easy to comprehend which devices were connected and what content was transferred."

Ory Janßen,
Head of IT
Stünings Medien GmbH

The risk of malware spread through USB devices

Nowadays, malware is a problem that affects Macs as well. Compared to Windows computers, the number of threats is still very low. However, the fact that malicious code which is able to bypass the security mechanisms of this usually very secure platform exists, shows the increased threat. Because of the growing spread of Mac OS X adoption in the industry, developing malware aimed specifically to Macs is getting more and more attractive.
With USB devices being a proven way to distribute malicious code, Stünings Medien started the evaluation of a Data Loss Prevention solution or, to be more precise, for the device control part of a Content-Aware DLP. „Controlling the (USB) ports will help us avoid the risks caused by employees using unauthorized, potentially infected smartphones or USB sticks at work. And besides that, we can make sure that no sensitive data is copied to these devices", says Ory Janßen, Head of IT at Stünings Medien GmbH.

Great features, simple management

The search for a product able to provide Device Control for Macs lead to a small amount of suppliers. Endpoint Protector 4 from CoSoSys was among the two solutions that were shortlisted and evaluated closely. The user-friendly interface and feature-based structure of Endpoint Protector was clear at first sight, providing the possibility to manage the software with ease. The amount of technical features for Macs - the control of USB and peripheral ports, as well as confidential content transfers – convinced Stünings Medien that Endpoint Protector was the right solution.
The possibility of creating whitelists to temporary use certain devices and especially the reporting and analysis features were considered extremely valuable. Stünings Medien decided to go with the Endpoint Protector 4 Virtual Appliance, specifically with the Device Control for Mac OS X module.
The setup of the appliance took very little time; the client software was enrolled to the endpoints from the server web-based user interface. Initially, Endpoint Protector was used for a few days to simply monitor and evaluate the logs related to USB devices. Them, the final policies were created according to the internal policy and compliance requirements. After a few months since Endpoint Protector has been protecting the Stünings Medien computers, Ory Janßen, the head of IT was truly happy with the implementation. His feedback can be seen as a valuable incentive for upcoming features of future releases.

>>

About Endpoint Protector 4

Endpoint Protector 4 protects Windows, Mac and Linux computers from data loss, data theft and data leakage by controlling all transfers to cloud-based applications and services like web browser, e-mail and Skype. The solution monitors the use of portable devices, for example USB sticks, CD/DVDs, HDDs or memory cards. Powerful security policies prevent data leaving the company through unauthorized exit points or by mistake.

Whitelist devices without network connection

The possibility of offline whitelisting devices meets the working processes at Stünings Medien. „Some employees are at the customers place frequently, presenting concepts and templates", explains Janßen. „They need to work with USB devices and transfer files even if their MacBook is not connected to the the company's' network." In this case, Endpoint Protector cannot check the connected device and decide whether it should be blocked. Therefore, the device will be blocked. However, by using the Offline Temporary Password feature which creates special permissions valid for a certain time period (between 30 minutes and 30 days), the employees' productivity is not affected.

One-click creation of reports

Furthermore, the intuitive and granular reporting is a big help. „With Endpoint Protector, we have the overview needed to evaluate the employees' activities. For example, it is easy to comprehend which devices were connected and what content was transferred.", stated Janßen. The policies of the company can be supported on a technical level by informing users about actions that do not comply with their access level or with the company policy. The decision of blocking or allowing a device can be done with high accuracy. Moreover, in the event of data loss or data leaks, which no security solution can avoid completely, the incident can be logged and reported. The IT administration can easily understand who transferred which data on what device. The log files help to prove that a certain data transfer leads to a data loss.

	Endpoint Protector GmbH	**CoSoSys Ltd.**	**CoSoSys USA**
E-Mail:	info@endpointprotector.de	sales@cososys.com	sales.us@cososys.com
Tel:	+49-7541-97826-730	+40-264-593110	+1-888-271-9349
Fax:	+49-7541-97826-279	+40-264-593113	

ENDPOINT PROTECTOR