



# Concentrate on Your Business Development by Ensuring Your Employees Do Too

August 2011

The larger a company becomes, the more difficult it is to keep track of what exactly each employee is doing during working hours. Without appropriate controls, you may find that people start uploading photos to Facebook, playing Farmville, or watching movies from a flash drive when they should be working. Of course, this impacts on employee performance and, as a result, business development. Moreover, this lack of discipline can also lead to IT security issues, e.g. targeted and zero-day attacks launched via vulnerable applications, infections from malicious websites, confidential data leaks from unknown USB flash drives etc.

What companies need is a convenient, easy-to-use tool that helps bring their employees' activities under control, increasing their performance and improving the overall level of IT security. Kaspersky Lab has developed Kaspersky Endpoint Security 8 for Windows, a new solution that not only protects corporate networks against all types of computer threats but also helps to centrally limit the use of non-business applications and removable devices as well as block access to unwanted websites.

The technologies implemented in Kaspersky Endpoint Security 8 for Windows have a number of advantages:

- ▶ Highly efficient due to seamless integration with other Kaspersky Lab technologies
- ▶ Easy management, including fine-tuning, from a single administration console
- ▶ Flexibility that supports security policies of any severity

## Application Control

Using Application Control, you can limit or block access to different categories of applications:

- ▶ Games (e.g. solitaire, poker, racing)
- ▶ Videos and music (e.g. Windows Media Player, Winamp Media Player)
- ▶ Instant Messengers (e.g. ICQ, QIP, Google Talk)
- ▶ Browsers (e.g. all, except Internet Explorer) etc.

To define an application category you can use dozens of pre-set categories or create them yourself. If there isn't enough information about an application to define its category, Application Control can send a request to the 'cloud'. The cloud-based reputation database contains information about more than 3 billion files and is constantly renewed. Over 300 million of the files are unique and make up the dynamic Whitelisting database.

Application usage can be limited not only by its category but also by user group. For example:

- ▶ Block Skype for everybody except the CEO
- ▶ Only permit the use of graphics editors (Adobe Photoshop, Microsoft Office Picture Manager) by the marketing department

---

The control policies can be adjusted for some applications limiting their usage, for example, during working hours.

Application Control is also an important component when it comes to securing a corporate network, due to multilevel checks of an application before its startup. Besides checks against whitelisting databases, applications are scanned by a heuristic analyzer, preventing possible malware infections. Finally, applications are checked by the on-access vulnerability scanner. When a vulnerability is detected, it can be shielded till the installation of the appropriate patch, preventing targeted and zero-day attacks from exploiting the breach.

## Device Control

As the name suggests, Device Control is capable of limiting the use of removable devices – flash drives, card readers, hard drives, cameras, mobile phones and other devices connected via USB cable, IR port or Bluetooth – on the corporate network. It means that employees won't be able to waste time on non-work-related activities using data brought from outside the office. Moreover, it makes it harder to copy confidential corporate data, e.g. contracts or databases, and intentionally or accidentally remove them from the office environment.

Devices can be blocked in different ways using the serial number (ID) of the device, device category (e.g. card readers) or connection type (e.g. USB bus).

Separate access rights can be applied to different user groups. For example:

- ▶ Block the use of flash drives in the finance department, with the exception of the CFO's flash drive
- ▶ Only allow the use of hard drives in the IT department
- ▶ Allow the CEO to use any type of device etc.

Control over the use of removable devices also enhances security, reducing the risk of viruses, spyware and other malware penetrating the corporate network via infected USB flash drives, hard drives and so on.

## Web Control

With Web Control you can block access to unwanted websites:

- ▶ Social networks (e.g. Twitter, Facebook, LinkedIn, VKontakte)
- ▶ Web mail
- ▶ Online games
- ▶ Internet TV etc.

Access to websites can be blocked not only by using their direct URL but also by using content filtering technology to prevent access to mirror sites. As is the case with the other types of control, different user groups can have their own access rights.

Some companies use separate gateway solutions to limit access to unwanted websites. However, this only works while a user is connected to the corporate network. As soon as an employee leaves the corporate perimeter, for example, on a business trip, the control policies are no longer applied. The risk of infection also increases, as malware is often distributed via social networks, web mail and other websites. Kaspersky Lab's solution works both inside and outside the workplace, maintaining a high level of employee output and ensuring protection no matter where you work.

## Corporate network management

All the control components are integral parts of the product and are easily managed via a unified administration console. The product offers a variety of settings for flexible access policies:

- ▶ The Default Allow scenario allows you to selectively block access to resources for all or some user groups
- ▶ The Default Deny scenario blocks any applications, removable devices and websites that are not authorized by the administrator in advance

---

Before implementing a new rule, it can be run in test mode. The test mode can help the administrator to understand the impact of any new rules on the system and to make adjustments to the parameters if necessary.

If you want your company to be focused on business development, you need to make sure your employees are concentrating on their work. With Kaspersky Endpoint Security 8 for Windows it couldn't be easier to create and centrally manage the optimal level of user activity control to increase the performance of your workforce and significantly enhance your company's IT security.