# Kaspersky
## Endpoint Security 8 for Windows®
## Control Tools

Kaspersky Endpoint Security 8 for Windows fuses powerful control tools into our existing anti-malware technology. Combined with Kaspersky's outstandng endpoint protection and an IT-friendly command center, Kaspersky controls are designed to keep businesses well ahead of emerging threats.

**Protection and IT policy enforcement through:**

- Application Control and Dynamic Whitelisting
- Web Content Filtering
- Device Control

## Application Control and Whitelisting Technologies

Two of the key innovations introduced in the Kaspersky Endpoint Security suite are the **Application Control** module and **Whitelisting** technology, which strengthen companies' security stance by enabling IT administrators to set policies that allow, block or regulate applications (or application categories).

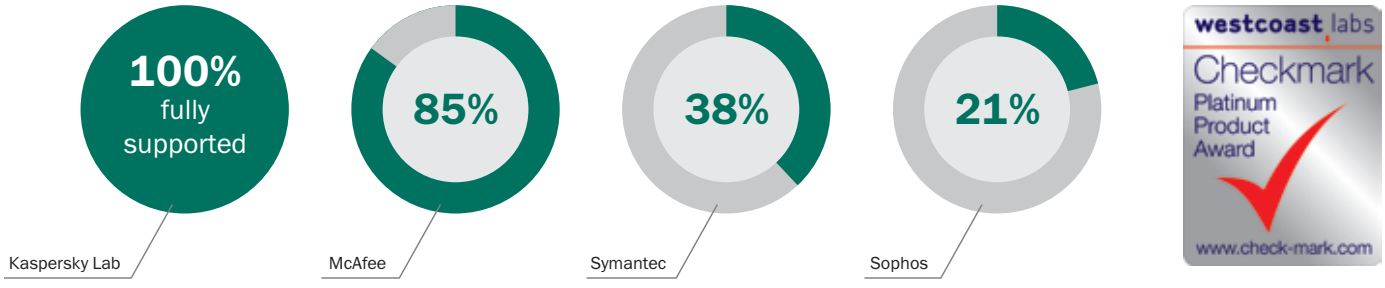
Kaspersky allows an organization to implement a **Default Deny** posture. In this scenario, all applications except those specifically allowed by the administrator are blocked by default. Kaspersky simplifies the administrator's work by grouping hundreds of millions of applications into categories for easy policy creation. The database of allowed applications can be created locally by the administrator or developed from the Kaspersky Lab categories.

As part of its Endpoint Security solution, Kaspersky Lab provides access to its dedicated **Whitelisting** database, which consists of programs that are constantly scrutinized to ensure they are legitimate. Kaspersky is the only security company that maintains a team of experts in a dedicated Whitelisting Lab!

Finally, Kaspersky's **Application Privilege Monitor** constantly watches and controls the behaviour of applications. Kaspersky can restrict whether an application can write to registries, what resources, such as storage, it can access, what user data it can control and modify, and much more.

### Default Deny test result

20 test cases in Total







Source: West Coast Labs, February 2012.

## Web Content Filtering

According to Google in June of 2012, about 9500 websites daily are identified as malicious. There are also multitudes of websites that contain material that's inappropriate for the workplace. For these reasons, it's important to use advanced web content filtering technology.

Kaspersky maintains a constantly updated directory of websites grouped by category (gambling, adult, research, etc). The administrator can easily create browsing policies around these categories — or customize them to create their own list. Malicious sites are automatically denied.

Policies can be set according to a schedule to allow browsing during certain times, and because Kaspersky integrates with your existing Active Directory structure, they can be applied across the organization quickly.

Kaspersky's innovative approach enables this technology directly at the endpoint. This means any policy you set will be enforced even when the user is off of the network.

## Advanced Device Control

Disabling a USB port doesn't always solve your removable device problems. Often, a more granular level of control is required to enable user productivity and security. For example, if a user must have a USB VPN token to access the network, but shouldn't be using USB removable storage devices — a "disable the port" policy won't work.

Kaspersky empowers the administrator to set policy and control any connected device, on any connection bus (not only USB), at any time. This means the administrator can regulate which devices can connect, read or write, the time of day a policy becomes effective, and which types of device are allowed. In fact, for extreme security, these controls can be managed right down the the specific device by individual serial number.

Because Kaspersky was built for the administrator, Device Control integrates with Active Directory, so setting blanket policies is simple and fast.

## Security Center

All these powerful controls are deployed through the Kaspersky Security Center — a straightforward, user-friendly command center which harmonises your IT security environment. The administrator can manage and control the security of all your physical, virtual and mobile devices from this single console.

To find out more about how Kaspersky controls work with our anti-malware technologies to secure your organization from cyber-threats and help make your business more agile and productive, speak to your solutions provider or contact Kaspersky.



KASPERSKY