KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Endpoint Controls

Kaspersky's powerful endpoint control tools are fused with our best-of-breed anti-malware technology to keep your business ahead of emerging threats.

APPLICATION CONTROL AND DYNAMIC WHITELISTING

Kaspersky's **Application Control with Dynamic Whitelisting** technology strengthens companies' security stance by enabling IT administrators to set policies that allow, block or regulate application (or application category) use.

Equipped with these technologies, organisations can painlessly implement a 'default deny' policy. In this scenario, all applications are blocked by default. The administrator then defines a list of applications allowed to run. 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 by leveraging the pre-defined Kaspersky Lab categories.

A module within this technology is **Application Privilege Control**. This module constantly watches and controls the behavior of applications. Kaspersky can restrict whether an application is able to write to registries, what resources, such as storage, it can access, what user data it can control and modify, and much more.

Finally, Kaspersky operates a dedicated **Whitelisting** database consisting of programs that are constantly scrutinised to ensure they are legitimate. In fact, we are the only security company that maintains a Whitelisting laboratory with its own dedicated team of experts!

WEB CONTROL

There are multitudes of websites that contain material inappropriate to the workplace. For these and other reasons, it's important to use advanced web controls.

Kaspersky maintains a constantly updated directory of websites grouped into categories (gambling, adult, research, etc.). Administrators can easily create browsing policies around these categories — or customise them to create their own lists. Malicious sites are automatically denied.

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

Kaspersky's innovative approach enables this technology directly at the endpoint. This means that any policy you set will be enforced even when the user is not on the network.

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 plug in a USB VPN token to access the network — but shouldn't be plugging in removable storage devices — a 'disable the USB port' policy won't work.

Kaspersky empowers the administrator to set policy and to 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 at which a policy becomes effective, and which types of device are allowed. For extreme security, these controls can even be applied to the specific serial number of the device.

EASY ADMINISTRATION

Because Kaspersky was built for the administrator, all controls integrate with Active Directory, so setting blanket policies is simple and fast. All of these endpoint controls are managed from the same console, meaning the administrator has a single intuitive interface that requires no additional training.

How to buy

Kaspersky **Control Tools** are not sold separately, but are enabled in these tiers of **Kaspersky Endpoint Security for Business**:

- Endpoint Security, Select
- Endpoint Security, Advanced
- Kaspersky Total Security for Business

CONTACT DETAILS

Not all features are available on all platforms
www.kaspersky.com.au/business

Download a free trial
www.kaspersky.com.au/trials