KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Endpoint Controls

Powerful endpoint control tools, tightly integrated with cutting-edge anti-malware and the industry's only dedicated Whitelisting laboratory helps protect your business from today's dynamic threat environment.

PROTECT, ENFORCE, CONTROL

Vulnerabilities in trusted applications, web-based malware and lack of control over peripheral devices form part of an increasingly complex threat landscape. Kaspersky Lab's Application, Web and Device Control tools enable complete control over your endpoints without compromising on productivity.

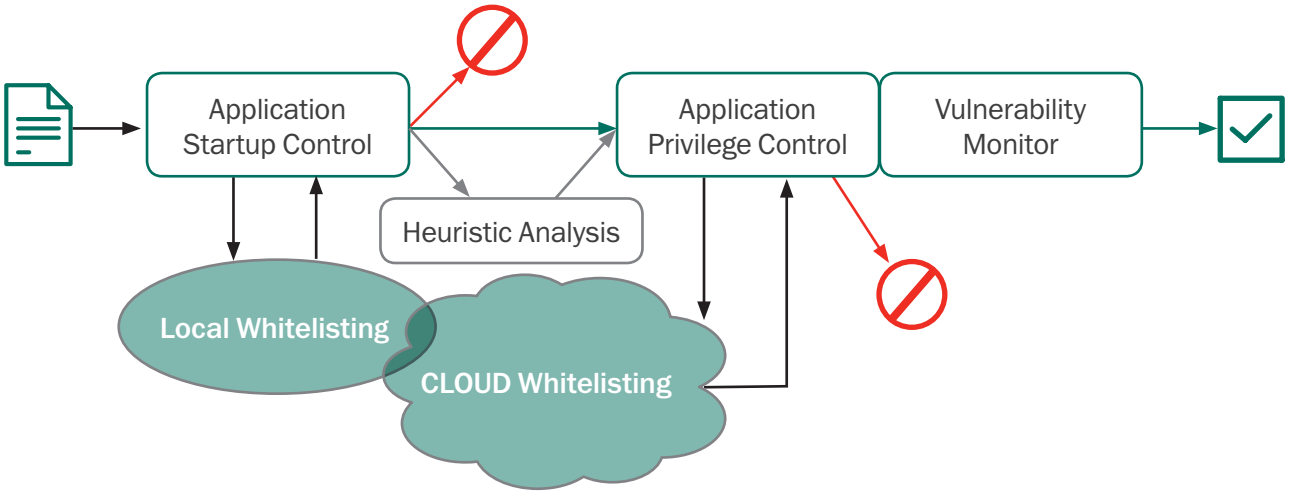
APPLICATION CONTROL AND DYNAMIC WHITELISITING

Protect systems from known and unknown threats by giving administrators total control over the applications and programs allowed to run on endpoints, regardless of end user behavior. In addition, enable application integrity monitoring to evaluate application behavior and prevent them from executing unexpected actions that could endanger the endpoint or network. Simplified, customizable or automated policy creation and enforcement enable:

- **Application start-up control**: Grant, block, audit application launches. Drive productivity by restricting access to non-business-related applications.
- **Application privilege control**: Regulate and control application access to system resources and data. Classify applications as trusted, untrusted or restricted. Manage application access to encrypted data on endpoints, such as information posted via web browsers or Skype.
- **Application vulnerability scanning**: Proactive defense against attacks targeted at vulnerabilities in trusted applications.

Most control solutions offer only basic blocking/access functionality. Kaspersky Lab's control tools are unique in their use of cloud-based whitelisting databases, enabling near-real-time access to the latest application data.

Kaspersky Lab's application control technologies use cloud-based whitelisting databases to analyse and monitor application at every stage: download, installation, execution.



Dynamic Whitelisting, which may be enabled via comprehensive 'Default Deny' blocks all applications attempting to run on any workstation, unless explicitly allowed by administrators. Kaspersky Lab is the only security company with a dedicated Whitelisting laboratory, maintaining a constantly monitored and updated database of more than 500 million programs.

Kaspersky Lab's **Default Deny can be applied in a test environment**, enabling administrators to establish application legitimacy before blocking. In addition, application categories based on digital signatures can be created, preventing users from starting legitimate software that's been modified by malware or comes from a suspicious source.

WEB CONTROLS

Monitor, filter and control the web sites that end users can access in the workplace, increasing productivity while protecting against web-based malware and attacks.

Kaspersky Lab's advanced web controls are built on a constantly updated directory of web sites, grouped into categories (e.g. adult, games, social networks, gambling,). Administrators can easily create policies to prohibit, limit or audit end user use of any individual sites or categories of site, as well as create their own lists. Malicious sites are automatically blocked.

By restricting their use, Kaspersky Lab's web controls help prevent data loss via social networks and instant messaging services. Flexible policies enable administrators to allow browsing at certain times of the day. Integration with Active Directory means policies can be applied across the organization quickly and easily.

For added security, Kaspersky Lab's web controls are enabled directly at the endpoint, meaning policies are enforced even when the user is not on the network.

DEVICE CONTROLS

Disabling a USB port doesn't always solve your removable device problems. For example, a disabled USB port impacts on other security measures, such as token-based VPN access.

Kaspersky Lab's device controls enable a more granular level of control at bus, type and device level – maintaining end user productivity while optimizing security. Controls can be applied right down to the specific serial number of the device.

- Set connect/read/write permissions for devices, as well as time scheduling.
- Create device control rules based on masks, eliminating the need to physically connect devices in order to whitelist them. Whitelist multiple devices simultaneously.
- Control data exchange via removable devices inside and outside the organization, reducing the risk of data loss or theft.
- Integrate with Kaspersky Lab's encryption technologies, to enforce encryption policies on specific device types.

EASY ADMINISTRATION

All Kaspersky Lab control tools integrate with Active Directory, so setting blanket policies is simple and fast. All endpoint controls are managed from the same console, through a single interface.

How to buy

Kaspersky Lab's Endpoint Control Tools are not sold separately. They are enabled in the 'Select', 'Advanced' and 'Total' tiers of Kaspersky Endpoint Security for Business.

KASPERSKY lab