Next Generation of Corporate Network Security

Today, malicious code spreads via websites, social networks, email as well as vulnerabilities in applications, and cybercriminals target companies of all sizes in order to steal money and confidential information In 2012 the total number of recorded web attacks exceeded 1.5 billion. Web-based attacks have increased at a similar rate to previous years. The number of attempted web-based infections in 2012 is 1.7 times greater than in 2011, while the number in 2011 was 1.6 times greater than in 2010. (Kaspersky Security Bulletin. Malware Evolution 2012).

In rapidly changing circumstances like these signature-based methods are no longer sufficient, as they block only known malicious files. The number of attacks has become so numerous that blacklisting technologies alone cannot cope. Something else is needed to boost security levels.

A variety of technologies and control tools are usually employed to enhance security:

▶ Application startup control
▶ Whitelisting
▶ Default Deny scenarios where all applications are blocked except those on a white list created by a system administrator
▶ Application privilege control
▶ Vulnerability assessment

There are pros and cons to all of these proactive technologies: improvements in the level of security often lead to an increase in resource consumption and false positives.

Such solutions are mostly the preserve of niche market players who claim that these technologies are a substitute for traditional signature-based analysis (blacklisting). This is unlikely to be the case in the near future because of the high cost of deploying and supporting a new system and also because signature-based methods are still the most effective when it comes to combating known malware.

Having failed to develop their own effective technologies, some companies end up buying a niche player's solution and combining it with their own technologies in a single product, managed from a centralized administrative console. Problems can arise when technologies with different origins fail to coordinate their work effectively. This can lead to system overload, potential incompatibilities as well as complicated settings and management of corporate IT security.

Kaspersky Lab has chosen a fundamentally different approach by developing its own Application Control and Whitelisting technologies and integrating them seamlessly with its other security components in the new Kaspersky Endpoint Security for Business.

How does Kaspersky Lab's solution work?

Before starting up, an application is checked by **Application Startup Control** against the **local Whitelisting database**, which is usually created by an administrator and contains information about the reputations and categories of known applications. If there is not enough information about the application in the local Whitelisting database, its metadata, containing nothing but a checksum of the file, is sent to be checked in the 'cloud'. The **dynamic Whitelisting reputation database in the cloud** contains information about hundreds of millions applications. More than 20 million users of Kaspersky Lab cloud services and 200 global partners update the database regularly and promptly. It provides access to information about new software that is released every day, minimizing false positives.

Based on local Whitelisting information and/or information from the cloud, a verdict about the application's **reputation** and **category** is generated. If all the data requested about the application is found, it is placed in a white list and assigned to one of the numerous categories: business applications, browsers, multimedia etc. If data about the application is limited or unavailable, it is placed in a grey list.

Based on the verdict it receives and in accordance with the **restriction policies** set up by the administrator, the application is either allowed to run or is blocked. Non-business-related software such as games or videos can be blocked for all or some groups of users.

The technologies implemented in Kaspersky Lab's solution allow highly flexible adjustment of corporate network protection. Besides numerous variations of the **Default Allow scenario**, **Default Deny scenarios** are also supported, allowing some of the strictest security policies to be applied. The administrator can permit the use of some application categories and prohibit all other applications.

Applications that are allowed to start up are then subject to **Application Privilege Control**, where any further actions can also be limited according to the administrative rules that can even block startup. In addition, grey applications are scanned by a **heuristic analyzer** for suspicious behavior.

In conclusion, all the applications undergo an **on-access vulnerability scan**. If the application turns out to be vulnerable, it can be shielded until the appropriate patch is installed, minimizing the risks of application backdoor attacks.

Advantages of Kaspersky Lab's solution

Application Control and Whitelisting from Kaspersky Lab provide multilayer protection from targeted and zero-day attacks and other computer threats. Because they were developed internally by Kaspersky Lab, all the solution's components are tightly integrated. This allows the most flexible adjustment of IT security for networks of any complexity with minimal impact on resource consumption.

KASPERSKY lab
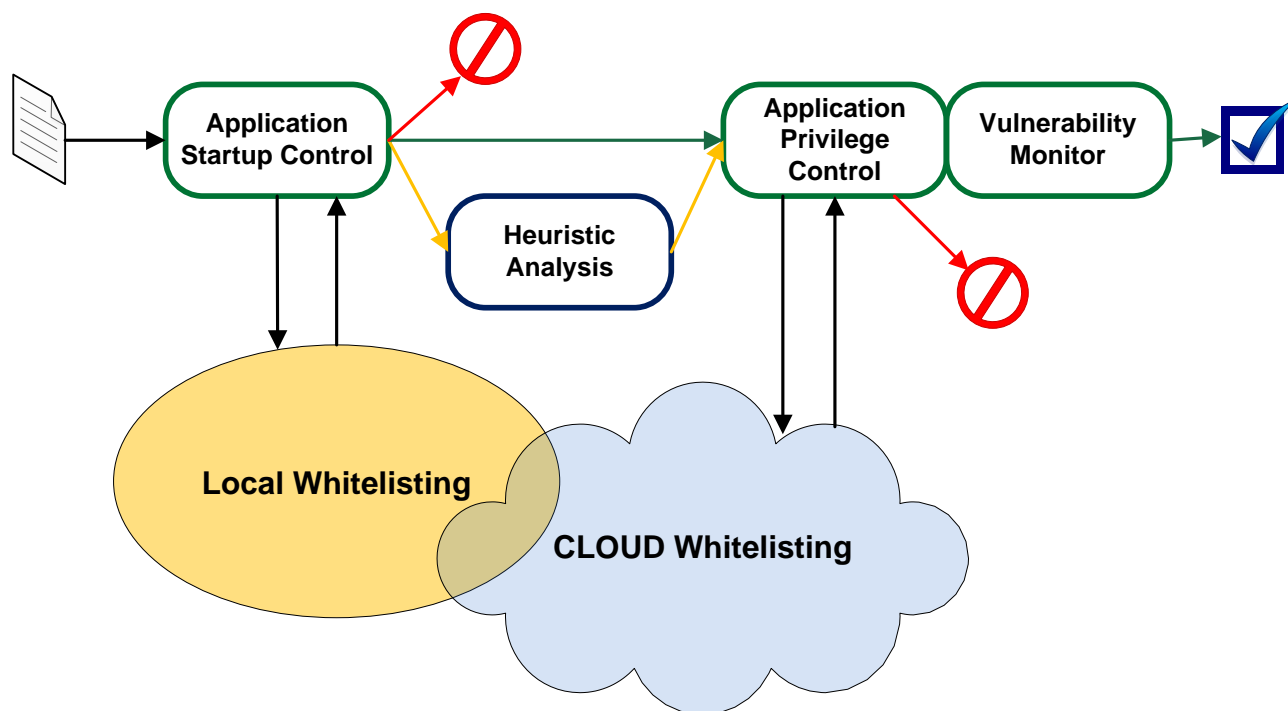
Application Whitelisting database

▶ Before implementation of any security policies, the software inventory can be used to automatically collect comprehensive information about the applications used across the corporate network

▶ The reputation base of Kaspersky Lab in the cloud contains information about more than 3 billion files and is continuously updated

▶ The dynamic Whitelisting database contains information about more than 300 million unique clean files and is growing by 1 million new files per day

▶ The status of applications already in the database is continuously tracked – the reaction to changes in an application's status is faster than that for other Whitelisting solutions due to all the technological infrastructure and expertise necessary for software analysis being concentrated within a single company

▶ Besides automated application scans, manual expertise is also used. The Virus Lab as well as the Whitelisting Lab, part of the Whitelisting & Cloud Infrastructure Research Department, constantly monitor database quality

▶ Information about software that is about to be released is received from more than 200 vendors, such as HP, Mozilla, Cisco, Adobe, Intel, and Asus, which helps minimize false positives

Application Startup Control

▶ Flexible software categorization: administrators can use a predefined list of categories from Kaspersky Lab, take them from the cloud or create their own list

▶ Software can be categorized by name, vendor, fingerprint etc. A "Golden Image" category containing programs that are required for booting the operating system can be created

▶ Integration with Active Directory allows the administrator to define application access rights for different groups of users

▶ Rule testing mode allows extensive information about the impact of a rule to be gathered before it is implemented

KASPERSKY lab

► Flexible adjustment of corporate protection: use of Default Allow or Default Deny scenarios and configuration of both an application's access level to system resources and the list of resources that must be protected from unauthorized access

Application Privilege Control & Vulnerability Scan

► Application Privilege Control can limit access of applications to critical system resources up to low-level access to the disk

► Vulnerability list is regularly updated during AV database updates

► Notification about detected vulnerabilities and vulnerability shielding with Kaspersky Lab technologies until the patch from the appropriate vendor is launched and installed

► Information about the latest vulnerabilities from Secunia, Microsoft and internal Kaspersky Lab databases

► On-access vulnerability scan when starting up an application

As the number of computer threats dramatically increases, new security technologies should be used alongside other security components to provide the necessary level of corporate IT infrastructure protection. Kaspersky Endpoint Security for Business combines Application Control, Whitelisting and other security technologies, developed internally and tightly integrated with each other, to provide the most efficient protection against all types of threats, especially targeted and zero-day attacks.

KASPERSKY⁑