Automating and Simplifying Security Administration Tasks with Kaspersky Systems Management

Today’s corporate IT infrastructure is a complex mechanism that requires constant maintenance and control. Special attention needs to be paid to the software components of that infrastructure: the operating systems, applications and email services, among others. System administrators must ensure that the entire network is stable, and that software programs are updated in a timely manner – a process which reinforces the company’s security. A single vulnerability in OS or application code can be used by cybercriminals to infect the company’s entire infrastructure and gain unauthorized access to confidential information. Such actions are often elements of a planned attack against a company designed to damage the company’s infrastructure, stop employees from working, steal corporate data, and generally cause as much harm as possible. According to a study conducted by B2B International and Kaspersky Lab in 2014, average losses caused by targeted attacks could cost $84,000 or more for small businesses, and $2,540,000 or more for enterprises. Furthermore, 12% of the IT professionals surveyed believed their organization had been the target of cyber-attacks during the previous year.

In order to automate and generally simplify for the IT department the process of accomplishing routine tasks, Kaspersky Lab has developed the Kaspersky Systems Management solution. It enables the remote monitoring and patching of software vulnerabilities, maintains the database of devices and software programs, and manages access rights within a local network, among others.

Kaspersky Systems Management capabilities

Kaspersky Systems Management provides centralized management for corporate IT security. It incorporates a number of management instruments that can significantly simplify the integration and maintenance of security solutions. The main system administrators’ assistant is Kaspersky Security Center – a single, unified management console that provides visibility and control of all of endpoint security technologies deployed in the corporate IT infrastructure. Kaspersky Security Center allows security to be managed on mobile devices, laptops, desktops, servers, virtual machines, and more. The system administrator has access to reports with detailed information on existing workstation vulnerabilities and is able to provide guidance on remediation actions. Moreover, these reports can provide an overview of the software status across the entire corporate network.

Thanks to the Role-Based Access Control feature, management responsibilities can be divided between multiple administrators and each administrator will only have access to the tools and information that are relevant to their responsibilities.

The main Kaspersky Systems Management features are grouped according to the functions they perform.

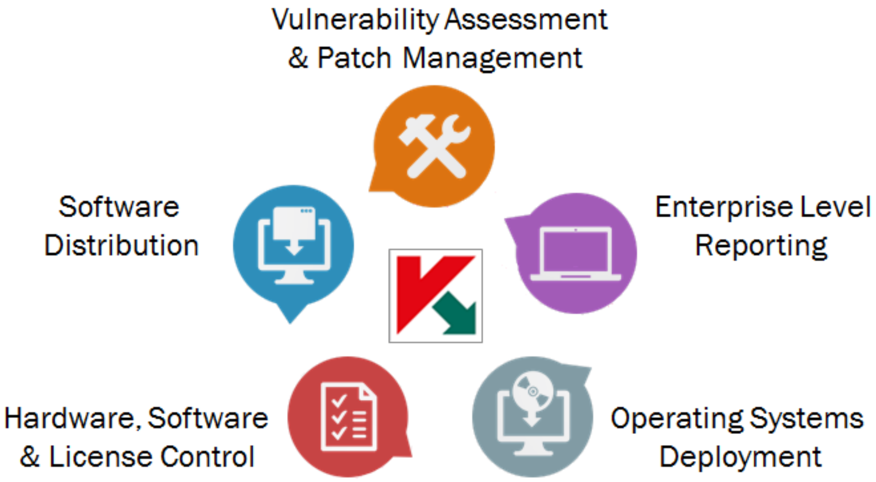
Vulnerability Assessment & Patch Management
Software Distribution
Enterprise Level Reporting
Hardware, Software & License Control
Operating Systems Deployment

Figure 1. Kaspersky Systems Management feaures

Vulnerability Assessment and Patch Management

The exploitation of vulnerabilities — such as errors in operating system code or applications — is one of the most common ways for cybercriminals to infect computers. Although finding a suitable vulnerability and writing malicious code (called an exploit) to take advantage of it may be a fairly complex task, malefactors continue to devote time and resources to this in the hope of profiting from successful data breaches. For this reason, scanning software for vulnerabilities that make a system more susceptible to infection remains one of the most critical elements of corporate and personal computer security. In order to tackle the task facing IT professionals: the search for, classification and patching of vulnerabilities in software installed on a company's infrastructure, Kaspersky Lab includes two specialized technologies in Kaspersky Systems Management.

Vulnerability Assessment technology

Vulnerability Assessment is a critical element in protecting a company against attacks involving vulnerability exploits, including targeted attacks. An IT department using Vulnerability Assessment can quickly detect vulnerabilities in corporate software that could potentially be exploited by cybercriminals, and can rapidly take action to eliminate those vulnerabilities.

A special software agent on the endpoint is used to detect vulnerabilities. It analyzes the versions of Windows OS present and other installed software, and then compares that data with data in Kaspersky Lab's vulnerability database. The information stored in this database is divided into three groups, depending on level of severity: Critical, High or Moderate.

This classification system helps system administrators to assess how up-to-date the software in the corporate network is overall, and to prioritize which updates and patches should be downloaded first. In addition to assessing the potential threat level posed by vulnerabilities, the database provides administrators with access to information concerning the potential impact of any exploit targeting the weak spot.

The Vulnerability Assessment component is designed to work alongside the Patch Management component. IT staff can obtain the data they need about recommended updates for specific vulnerabilities via the centralized administration console; then start making immediate plans for update installation.

Patch Management technology

The Patch Management technology is used to update software installed on Windows workstations, patching vulnerabilities and boosting the level of protection. Once the Vulnerability Assessment has found a vulnerability on the workstation, and its software developer has already released the appropriate patch, it is downloaded to the company's local server and installed on all workstations running that software. The software update process can be initiated manually by the systems administrator, or can be set up for automatic updates using Kaspersky Systems Management. For example, updates can be scheduled to take place during non-business hours to avoid interfering with day-to-day work.

Patch Management can update software developed by various vendors. In the case of Microsoft Windows, it communicates with the Windows Update service to keep OS components up to date. It also features the ability to use the company's server for Windows Server Update Services (WSUS).

These technologies keep IT professionals informed of all of the latest changes in the company's software environment and allow them to control the download and installation processes without leaving their own workstation.

Hardware, Software and License control

Kaspersky Systems Management uses data from the Windows registry to collect information about each computer's hardware and the software installed on it. This data helps administrators to track the status of company devices and to control and analyze employee software usage. It also supports the management of existing software licenses, ensuring they are all up-to-date and in active use. In other words, Kaspersky Systems Management helps maintain a complete database of all IT assets, and can quickly show system administrators the owner of each hardware piece or number of physical cores in the exact CPU.

Another useful instrument that helps to control devices in the corporate network is the Network Access Control. This component of Kaspersky Systems Management provides the tools to set up policies for guest device connection to the corporate network. It allows access to the corporate network to be restricted for unsafe devices that do not comply with security policy criteria, and provides transparent access to the network for protected corporate devices. The administrator can choose to limit guest device access to specific nodes or to block the connection completely, boosting the security level of the overall infrastructure. Guest devices can be automatically detected and redirected to the guest portal as well as being provided with Internet access.

Software Distribution

Kaspersky Systems Management also allows system administrators to remotely install applications on computers within the corporate network. Background installation is supported to minimize interference with user performance. In addition to the standard MSI packets, this component works with *.exe, *.bat, *.cmd and similar file types. Administrators can also initiate installation with additional special parameters.

To make administration of the network in remote offices even simpler and not to overload the network channel, Kaspersky Systems Management enables software to be renewed through one of the remote workstations. This can be designated an Update Agent, and will be updated first, with later installation packages distributed to the rest of the office via the local network. This optimizes the Internet traffic, which is especially important for large networks.

In addition, Systems Management provides a means for remote connection to the desktop of any corporate computer via a secure tunnel. This remote troubleshooting connection allows the administrator to solve problems without leaving their desk and reduces the number of inefficient telephone conversations with end users. Permission should be received to connect to the computer, while all the actions are being logged to provide a secure and compliant connection.

Operating Systems Deployment

System administrators can create an image of the OS installed on any workstation within the local network and use it to install the operating system on other endpoints. This approach helps keep all computers up-to-date just by updating the master image, which can be easily edited.

Deployment of the images can be made with either PXE servers (Preboot eXecution Environment) or using Kaspersky Systems Management's own features. To have the opportunity to distribute the images after office hours, Kaspersky Systems Management supports Wake-on-LAN signal sending.

Enterprise Level Reporting

Another feature that will be of assistance for enterprise-level businesses is compatibility with external Security Information and Event Management (SIEM) Systems, namely HP ArcSight and IBM QRadar. It allows system administrators to monitor security alerts generated by network hardware and applications.

Advantages

The technologies included in Kaspersky Systems Management are designed to:

- Automatically search and close vulnerabilities in company software;
- Facilitate easy integration with existing IT infrastructure and provide a worry-free connection of new users and devices in future;
- Provide additional protection for the company's infrastructure by controlling software and hardware, including guest devices;
- Help system administrators carry out routine tasks, and provide broad capabilities for automating processes and a convenient means of centralizing security management;
- Contribute to company savings through increased resource efficiency, reduced impact on user activity and potential cost savings through identifying superfluous software licenses;
- Provide detailed reports on existing vulnerabilities and installed updates.

Availability

Systems Management is available as a part of the following products for business users:

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

It is also available as a stand-alone targeted security solution:

- Kaspersky Systems Management