

Kaseya Endpoint Security - KES

Extend the IT services process by including centrally controlled security protection.

KES, a powerful and proven add-on to the Kaseya IT Automation Framework, enhances and extends support for the IT delivery process by including an essential security protection component. By incorporating reactive anti-virus and spyware detection with the latest proactive technologies, IT Professionals are able to expand their service offering to include effective protection against malicious programs ensuring not only anti-virus protection but protection from unknown threats.

Anti-Virus protection from Viruses, Worms and Trojans

■ Analyze

Analyze and detect unwanted executable applications or DLL libraries within the system that may be spyware, adware etc. Based upon the security profile, KES will remove these programs or block access to them.

■ Scan

Scan the system registry for suspicious entries, temporary Internet files and tracking cookies, and treat the potentially harmful items in the same manner as any other infection.

■ Detect computer viruses by:

- **Scanning** – on-access and on-demand scanning
- **Heuristic Analysis** – dynamic emulation of a scanned object's instructions within a virtual computing environment
- **Generic Detection** – detection of instructions characteristic of the virus or group of viruses
- **Known Virus Detection** – searching for character strings characteristic of a virus

Multi-Level Virus Checks:

■ E-mail Scanner

Checks incoming and outgoing mail by using plug-ins designed for the most frequently used e-mail programs. The E-mail Scanner is an additional program for electronic mail monitoring and is designed for applications supporting the POP3/SMTP protocols. Once detected, viruses are cleaned or quarantined. Some e-mail clients may support messages with text certifying that sent and received e-mail has been scanned for viruses. In addition, for an increased level of security when working with electronic mail, the Attachment Filter can be set by defining undesirable or suspect files.

■ Real Time Protection

Scans files as they are copied, opened or saved. When the Real Time Protection discovers a virus in a file that is accessed, it stops the operation currently being performed and does not allow the virus to activate itself. The Real Time Protection, loaded in the memory of the computer during system startup, also provides vital protection for the system areas of the computer.

■ On-Demand Scans

Scanning is a crucial part of KES functionality. Scans can be run on-demand or scheduled to run periodically at convenient times. KES comes with pre-defined security profiles along with the ability to create customer profiles.

■ Anti-Spyware

Spyware is usually defined as a type of malware (software that gathers information from a computer without the user's knowledge or consent). Some spyware applications may also be deliberately installed and often contain advertisements, window pop-ups or different types of unpleasant software. Ideally, spyware and other malware should be prevented from intruding. Currently, the most common source of infection is websites with potentially dangerous content. Other methods of transmission include e-mail



Kaseya Endpoint Security Key Benefits

- Extends your IT service capabilities
- Complete integrated solution that provides security protection for desktops, notebooks, and file servers
- Central administration of all features, including deployment updates, and scheduling
- Reduced costs and purchasing requirements
- Easy to use protection – install and forget
- Proven by all major antivirus certifications (VB100%, ICSCA, West Coast Labs Checkmark)
- Improved virus detection based on better heuristics and NTFS data streams scanning
- Unique automatic threat-removal anti-spyware engine
- Real-time protection with on-access scanning



Our Automation. Your Liberation.™

www.kaseya.com

or transmission by worms and viruses. The most important protection is to use an always-on background scanner, such as the cutting edge KES Spyware component. It works like a resident shield and scans applications in the background as they run.

■ Centralized Management

Centrally managed security profiles are defined and deployed to the managed computers using the Kaseya console interface. The profiles are used to establish best practices to keep the managed computers running and malware free. All information detected is logged within the system and available for executive summary and detailed management reporting.

■ Automated Deployment

As a fully integrated component of the Kaseya IT Automation Framework, KES is configured, deployed and managed from the same Kaseya interface that administrators already use to manage their computing environments, making implementation seamless and easy. Once deployed, the system is monitored to ensure protection is active and enabled. Utilizing the Kaseya proactive practice, updates are handled automatically on a scheduled basis without the need for user interaction. Security protection is then always up and running and kept up-to date. All activity and information detected is logged and stored in the Kaseya database and is available for executive summary and detailed management reporting.

■ Virus Detection

The Scanning engine has received numerous awards for its excellent detection of "in the wild" viruses, including the VB100% award. Its unique combination of detection methods provides full protection against viruses, worms and trojans.

■ Cutting-Edge Anti-Spyware Technology

Detects spyware, adware, DLL-trojans, keyloggers, and much more. Malware hidden in data streams, archives, or the Windows registry is also detected.

■ Full On-Access Protection

Provides maximum protection by scanning every file opened, executed, or saved. It also prevents the opening or executing of infected files.

■ Flexible Intelligent Scanning

Is used to include/exclude files from being scanned based on individual file extensions and can handle exceptions for potentially unwanted programs such as adware.

■ Full E-mail Protection

Checks every e-mail sent or received, providing full protection from e-mail-borne threats. Supports MS Outlook.

■ Automatic Threat Handling

Automatically heals or removes infected files and other threats such as trojans, worms and spyware.

■ Powerful Scheduling

Automatically provides recommended daily schedules for scanning and updating, and allows you to create custom-scheduled events.

About Kaseya

Kaseya is the leading global provider of IT automation software for IT Solution Providers and Public and Private Sector IT organizations. Kaseya's IT Automation Framework™ allows IT Professionals to proactively monitor, manage and maintain distributed IT infrastructure remotely, easily and efficiently with one integrated Web based platform. Kaseya's technology is licensed on over three million machines worldwide.

For a free 30 day trial visit www.kaseya.com/download

Contact Kaseya: www.kaseya.com | sales@kaseya.com

Copyright ©2009 Kaseya. All rights reserved. Kaseya, the Kaseya logo, Our Automation, Your Liberation and Kaseya IT Automation Framework are among the trademarks or registered trademarks owned by or licensed to Kaseya International Limited. All other brand and product names are or may be trademarks of, and are used to identify products or services of, their respective owners.

The KES Anti-Virus/Anti Malware solution is backed by the award winning AVG technology. AVG possess a strong and respected technology background. With over 40 million users, AVG has worldwide recognition in the Anti-Virus market and plays an active role in the security software industry. In 2005 AVG was accepted to the Anti-Spyware Coalition (ASC), an organization of software companies, academics and consumer groups working together to combat spyware and other malware threats.

Agent Requirements

- 333 MHz Pentium-class CPU or greater
- 128 MB of RAM
- 30 MB of free disk space
- Network Interface Card (NIC) or modem
- Microsoft Windows 98, Me, NT 4.0, 2000, XP, Vista, Server 2003
- Macintosh OSX v10.3.9 and above, Intel and PowerPC editions
- TCP/IP Outbound Port 5721
- No Inbound Ports

Minimum Kaseya Server Requirements

- Single processor (1.0 Ghz, 160 Mhz front side bus, 1 MB cache)
- 1 GB RAM
- 40 GB hard drive
- Microsoft Windows Server 2003
- Microsoft Internet Information Server (IIS) version 5 and up
- Microsoft SQL Server 2005 (or 2000) or SQL 2005 Express Edition (included in standard download)
- Cannot be installed on a server running Microsoft Exchange
- 100 Mbps Network Interface Card (NIC)
- DSL or Cable modem internet connection
- TCP/IP open ports: 80 inbound and outbound, 5721 inbound



Our Automation. Your Liberation.™

www.kaseya.com