

Kaspersky provides robust AV

REVIEW: BUT SOLUTION NEEDS BROADER REPORTING FUNCTION

By Andrew Garcia

KASPERSKY LAB'S KASPERSKY ANTI-VIRUS 6.0 is a robust desktop security solution that's backed by a lightning-fast security response team and a seemingly endless supply of signature updates.

However, while the product's management platform performs its core duties satisfactorily, we'd like to see Kaspersky widen the scope of the software's reporting capabilities—either through internal development or third-party partnerships.

Although the product is called Kaspersky Anti-Virus, this name singles out only one of the several layers of security defense that Kaspersky has bundled into its offering. The product automatically defends against viruses, Trojans and hack tools, plus other spyware and adware.

Kaspersky Anti-Virus 6.0 also includes a desktop firewall as well as intrusion prevention defenses that block an attacking computer for a specified period.

For Web defenses, Version 6.0 includes an HTTP protocol-scanning engine, anti-phishing and anti-banner functions, and a pop-up blocker. The software also offers mail defenses with incoming and outgoing protocol scans and mail-store detection.

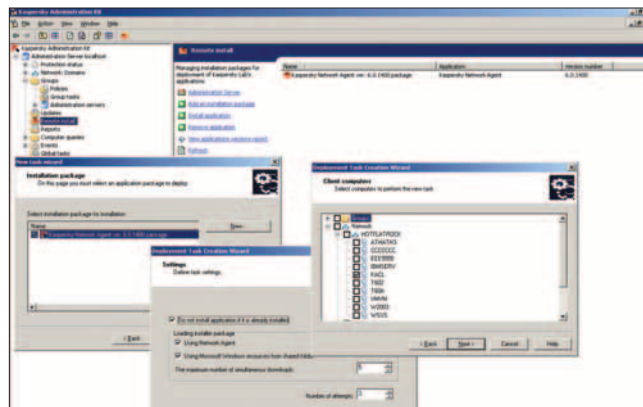
Rootkit detection, system hook detection and a registry monitor round out the vast array of protection services.

Kaspersky Lab offers enterprises four tiers for Anti-Virus 6.0, with versions designed for workstations, file servers, mail servers and Internet gateways. eWEEK Labs tested the Workspace Security tier—which includes workstation protection for the Vista, XP, 2000, ME, 98 SE and NT 4.0 Workstation versions of Windows, plus several Linux and BSD distributions—and the central management platform called the Admin Kit. Pricing for the Workspace

Security tier sells for about \$12 per protected node.

In a centrally managed environment, Kaspersky's workstation client has two distinct components. First, there's the anti-virus client, which handles all security detection, cleaning and blocking. Second, there's the network agent, which processes updates, policies and job requests from the Admin Kit and issues alerts and status updates. Combined, the two components are fairly lightweight when it comes to resource utilization, with three processes consuming about 12.5MB of RAM with the software at rest.

In our malware tests, Kaspersky Anti-



From the Admin Kit, we could easily deploy the Network Agent or AV engine.

Virus 6.0 did only marginally better than Microsoft's FCS (Forefront Client Security), thwarting 21 of our 29 samples—detecting 19 malware strains along the way. Interestingly, Kaspersky Anti-Virus 6.0 and FCS agreed on only 12 of our infected bundles.

We did notice one glaring false positive during our tests, however, as Kaspersky's software attempted to isolate the touch-pad driver that came with our test laptop.

Kaspersky Anti-Virus 6.0 offers centralized management through the free-to-customers Admin Kit, which can be installed on either a Windows-based server or workstation operating system. The Admin Kit

offers a one-stop shop for agent, policy and update distribution; policy creation; and alert monitoring.

However, the Admin Kit lacks the wider scope of security-posture visibility that we found with Microsoft's FCS. Kaspersky Anti-Virus 6.0 serves anti-virus views up to Cisco's NAC framework, but we would like added support for the NAC schemes of Microsoft and the Trusted Computing Group for wider coverage.


From the Admin Kit, we could easily automate distribution of security components and policies to clients. Within the Admin Kit console, which has the familiar feel of an MMC (Microsoft Management Console) snap-in, we created managed groups to which we assigned security policies.

Kaspersky bases its company's reputation on its ability to create and deliver threat signatures faster than anyone else.

To uphold this pledge, Kaspersky offers frequent updates—practically on an hourly basis. In comparison, Microsoft's FCS offered new signatures three to six times a day.

As a result, Kaspersky Anti-Virus 6.0 requires an efficient delivery system to get the updates to the Admin Kit, which then pushes them to the managed clients. To help prioritize updates, we created different download

policies that checked for threat signature updates every half-hour, and another policy that checked for other signature types and client module updates on a less frequent basis.

This helps reduce the amount of network bandwidth depending on the type of update. We could configure the system to check Kaspersky's servers for threat signatures every half-hour, while creating another policy to update other components less frequently. 

Senior Technical Analyst Andrew Garcia can be reached at andrew_garcia@ziffdavis.com.

Reprinted from eWEEK, May 28, 2007 with permission from Ziff Davis Media Inc.

©2007 Ziff Davis Publishing Holdings Inc. All rights reserved.