

Quick Facts about Kaspersky Endpoint Security 8 for Windows:

Platforms Supported:
Kaspersky Endpoint Security 8 for Windows runs on both workstations and servers

Final Beta available:
September, 2011

Public Launch Date:
October, 2011

Upgrades:
Customers with valid licenses of Kaspersky Open Space can enjoy free upgrades to this new version.



For more information please contact our Inside Sales Team at corporatesales@kaspersky.com

www.kaspersky.com

Sneak Peek Series

What's New in Kaspersky Endpoint Security 8 for Windows?

In October 2011 Kaspersky Endpoint Security 8 for Windows will be released as Kaspersky's flagship endpoint protection suite. The new release offers comprehensive security for both physical and virtual environments providing protection from today's evolving security threats.

In addition to the award-winning technology built into every Kaspersky product, Kaspersky Endpoint Security 8 for Windows includes powerful features that dramatically improve business security and the administrator's control tools.

Improved Protection:	
New Detection Engine	Vastly improved malware detection and reduction of false positives in file, mail and web traffic.
Kaspersky Security Network	Integration with KSN provides rapid protection from emerging threats based on analysis of real-time activity from the global Kaspersky user community.
System Watcher	An intelligent module that proactively monitors and analyzes system operations for suspicious activity.
Behavior Stream Signatures Technology	Identifies dangerous application patterns within a users system.
Whitelisting and Cloud-Based File Reputation	Kaspersky's cloud-based file reputation database contains billions of known and safe executables that further protect the system from malicious code and reduce false positives.
Rollback of Malicious Activity	Automatically reverts a system to a point before malicious activity occurred.
Advanced Firewall and Intrusion Detection System	Kaspersky's flexibly managed firewall and IDS align with your application control policies to improve employee productivity.
Vulnerability Scanning	Avoid potential exploits by identifying system weak points, missing patches and neglected application and OS updates.
Enhanced Control Tools:	
Device Control	Granular control of device operations, reducing the risk of data loss and enforcing usage policies.
Application Control	Applies restrictions to various actions of applications in the operating system as well as rights to access system resources.
Application Startup Control	Provides administrators the ability to grant, block and audit application launches.
Web Control and Content Filtering	Monitoring and filtering users' browser activities by category, content and data type regardless of workstation location.