



ENTERPRISE SECURITY Complete online security suite for your business.



Businesses all over the world have a compelling reason to identify and address growing number of vulnerabilities - Buffer overrun, Identity spoofing, Elevation of privilege, Information disclosure, Denial of service, to name a few. K7 developed a world class solution to help businesses eliminate these threats - K7 Enterprise Security

K7 Enterprise Security also protects your business from unknown security threats and from various risks tied to the extensive usage of social media, by allowing Administrators to have full control over the Endpoints at all times. This is achieved by taking advantage of the features highlighted below.



KEY HIGHLIGHTS

Web based Management console accessible from within the network using standard Web Browsers:

- > Single Console to control Servers & Endpoints.
- > Simple and quick deployment of endpoint protection remotely.
- > Active directory support for endpoint protection deployment.
- > Dashboard to provide quick view of Endpoints.
- > Email notification of security events whenever administrator attention required.
- > Grouping of Endpoints for easier management, multiple policies to customize security settings for Endpoints.
- > Policy override facility to implement security changes across all Endpoints without having to change all the policies.
- > Remotely scan / update / restart / uninstall any Endpoint at any time.
- > Control web access of Endpoints using advanced web filtering.
- > Control external device access of Endpoints.
- > Control Endpoints application access privileges - launching / accessing the internet.
- > Set automatic security policy for travelling laptops.
- > Simple & comprehensive security reports.
- > Centralized Quarantine.
- > Targeted remote malware cleanup.
- > Multiple client / endpoint security support - Business Servers, File Servers, Desktops, Laptops.
- > Stealth mode keeps the system invisible while connected to the internet.
- > Provides suggestions on the network profile you could assign while connecting to any new network.
- > No notifications, automatic decision making when any trusted Windows application connects to the Internet.

Real-time Anti-Virus Protection:

- > Proactive real-time scanning ensures all new files accessed, downloaded, created or modified are automatically scanned.

Email protection:

- > Email protection automatically scans all incoming and outgoing e-mails and blocks malicious attachments, protecting the Endpoints from e-mail based virus and malware attacks.

Proactive defense mechanism:

- > **Zero Day protection:** Prevents Endpoints from any zero day attack and from PDF or browser based exploit. Endpoints don't have to wait for a patch addressing these exploits.
- > **Behavioral blocking:** Blocks and removes any new malware based on behavioral analysis undetected by traditional AV.
- > **Drive-by-Download blocking:** detects and blocks zero day browser exploits leading to drive-by-download and rogue AV download.
- > **External device Access control:** (read / write / execute access) Access to USB sticks, CD, DVD and Floppy drives set by Administrator gets instantly reflected on Endpoints.

Root-kit scanner:

- > Detects and removes any root-kit hidden on Endpoints using advanced detection technology.

Vulnerability detection:

- > This feature detects vulnerable application modules that can be used by attackers to compromise Endpoints.

USB Vaccination:

- > This feature can be used on any individual USB drive. Vaccinating the USB device ensures it never gets infected even if used on an infected PC.

Smart Firewall:

- > Automatically detects the current location of Endpoints (in-office or out-of-office) and applies appropriate security rules by taking into account security risks outside the network. Intrusions are also detected and blocked.

Application Control:

- > Restricts launch of any application or blocks network and internet access of applications.

Web Filtering:

- > Prevents Endpoints from accessing certain websites set by the Administrator based on categories (e.g. Social media, gambling,...)

Up-to-date Protection:

- > Updates are downloaded from the centralized server enabling faster deployment of updates and saving bandwidth. Mobile laptops download updates from the internet when outside the network.

NANO SECURE TECHNOLOGY

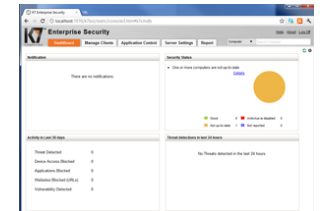
NST

Nano Secure Technology

- > Nano Secure Technology is the next generation Security Software CORE
- > Enables prudent security solutions in multiple layers analyzing & collating various events to detect and block threats



Admin Console - Dashboard:



Endpoint Security:



System requirements for Administrator Console:

- Operating Systems:**
Windows Server 2003 (SP1 or later) - Any edition
Windows Server 2008 - Any edition
Windows Small Business Server 2011 - Any edition
Windows XP (SP2 or later) / Vista / Windows 7
- Web Browsers:**
Internet Explorer 8 or later
Firefox, Google Chrome, Safari
- Hardware:**
512 MB RAM
700 MB hard disk space (incl. database)

System requirements for Endpoint Security:

- Operating Systems:**
Windows Server 2003 (SP1 or later) - Any edition
Windows Server 2008 - Any edition
Windows Small Business Server 2011 - Any edition
Windows XP (SP2 or later) - 32 bit only / Vista / Windows 7
- Hardware:**
512 MB RAM
400 MB hard disk space

