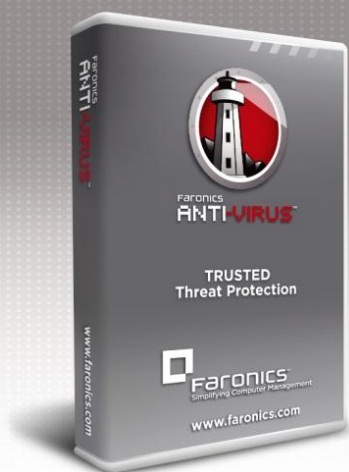# Product Spec Sheet
## Faronics Anti-Virus

### System Requirements

Faronics Anti-Virus works with computers running Windows XP SP3 or later (32 and 64 bit), and Windows Vista SP1 (32 and 64 bit), Windows 7 (32 and 64 bit) Windows Server 2003 and 2008 (32 and 64 bit). Information on Faronics Core system requirements can be found in the Faronics Core user guide.

## High Performance Technology

- The MX-Virtualization™ engine analyzes malware in real-time, observing its behavior before it can actually infect the computer– ensuring zero-day threat detection
- Advanced anti-rootkit technology finds and disables dangerous hidden processes, modules, services, and files
- High speed file scanning
- Low CPU and memory usage during scans
- Efficient, continuous virus definition updates (at least two daily)
- Regular threat-engine updates
- USB devices are automatically scanned upon connecting
- Option to exclude folders and files from scans

## Centralized Management & Integration

- Faronics Core provides a secure platform to manage anti-virus protection (definitions and threat-engine updates) across the enterprise
- Configuration and scan scheduling done via "policies" that are centrally applied to workstations
- Virus definition updates are managed and hosted on Faronics Core Server
- Full global or workstation-specific threat reporting available via Faronics Core Console
- Out-of-the-box compatibility with Faronics Deep Freeze and Anti-Executable to provide a solid "layered security" strategy
- Ability to import/export anti-virus policies

## Advanced Protection

- Email protection works on top of any POP3- and SMPT-based email program including Microsoft Outlook
- Embedded firewall can configure specific network ports access
- Host Intrusion Prevention System allows processes to be protected by preventing one program from injecting code into another program
- Intrusion detection system blocks malicious programs based on incoming and outgoing traffic analysis

## www.faronics.com

AV3-0_V1_Datasheet_EN