

**Rudra** Is Tomorrow's Technology, That You Needed **Yesterday**

Rudra - Detecting  
UnKnown Computer  
Viruses - A New  
Approach

The logo for Rudra, featuring the word "rudra" in a lowercase, sans-serif font. Above the letter "a" is a stylized flame icon.

[www.rudratec.com](http://www.rudratec.com)

## RUDRA - INTRODUCTION

Rudra technology protects computers from Viruses, Worms, Spyware, and other Malware in their UNKNOWN state.

Since today's society is more and more dependent on computer networks—in personal communications, corporate activities, and the overall infrastructure—we are seeing an increasing risk of serious damage from computer viruses. Antivirus programs are now installed in computers as a matter of course; however, conventional antivirus software relies on pattern matching based on a database of known viruses and therefore is ineffective in detecting unknown viruses.



Rudra patent pending technology is a unique technology that does not use any signature database and requires no periodic updates. It offers comprehensive protection against viruses, worms, spyware and other malicious software - which will be created in future, providing your computer a total and complete protection from malware.

### Prevention:



The increasing sophistication of viruses and its variants has led to higher risk of infection, and has increased the efforts in pattern extraction to cope with such variants. Since these infections can cause immediate and serious damage,

Rudra fills this gap with an accurate detection technology that can prevent this damage by detecting unknown viruses.

Today, the most common sources of virus infection include e-mail, virus propagation through shared disks in computer networks, and websites with potentially dangerous content.

## Rudra – Pioneering a new Revolution

Now, for the first time Rudra Technologies Pte Ltd, presents RUDRA a paradigm shift in anti-malware technology. Rudra is the first step towards providing comprehensive protection from all malware. Moreover, Rudra does not need constant updates.

### What makes Rudra unique?



Today, the most common sources of virus infection are emails, shared disks in computer networks and websites with potentially dangerous content. So your system is perennially under attack. At any given moment, there are numerous “unknown viruses” prowling the Internet. In fact, your next click could be fatal to your system.

Rudra unique technology is neither signature based nor heuristic. Instead it simply focuses on making your system “malware unfriendly” and constantly protects your core content from intruders.





Malware is the short name for “Malicious software” which is usually designed to damage or disturb a system. These include – Viruses, Worms, Wabbits, Trojans, Backdoors, Spyware, Exploits, Rootkits, Key loggers, Dialers and URL injections.

### So how does Rudra Protect?

To make your system invulnerable, Rudra does not restrict itself to recognizing known



viruses (like signature and heuristic technology). It simply focuses on making sure that the malware cannot run on your system in order to cause any damage by:




-  Enhancing system security and integrity by preventing execution of known and unknown malware
-  Increasing up-time on PC's and laptops
-  Reducing time spent on activities caused by malware (e.g. viruses, Trojans, worms etc)
-  Protecting from present, past and future viruses and other malicious software



Rudra's propriety technology ensures that no virus remains undetected long enough to start running. Rudra differentiates between legitimate executables and malware. It captures the malware as soon as it enters and installs and does not wait till it starts executing. Moreover, Rudra provides dual protection by preventing access to RAM by unauthorized programs.

|                    | Rudra | Existing Anti-Virus Technologies   |
|--------------------|-------|--|
| Scanning           | X     | Searching for character strings, typical of a given known virus                          |
| Heuristic Analysis | X     | Dynamic emulation of the scanned object's instructions in a virtual computer environment |
| Generic Detection  | X     | Detection of instructions characteristic of the given group of virus                     |
| Integrity Check    | X     | Tracking of changes that occur in the scanned objects as you use your computer           |

Many commercially available antivirus programs apply a detection system based on the “pattern (signature) matching” or “scanner” method. This system extracts certain binary code segments from known viruses, enters them into a database in the form of hexadecimal strings (called “patterns” or “signatures”), and matches files against this database to determine whether they are viruses. Generally, this system has the following disadvantages:

-  The system cannot detect unknown viruses whose patterns are not contained in its database.
-  It is difficult to create patterns that can uniquely characterize viruses and prevent safe files from being misidentified as viruses.
-  Existing patterns are rendered inapplicable to matching simply with partial modification of the virus code (as seen in numerous virus variants)—in an extreme example, this can be accomplished merely through recompilation of the code with a different compiler.











In addition to matching of simple string patterns, antivirus vendors are now developing more common patterns that can include

regular expressions instead of simple character strings, as well as pattern matching using file or program structures. However, these matching methods essentially rely on syntactic information and are thus fundamentally limited.




To detect unknown viruses, some antivirus programs apply the “dynamic protection” process, in which suspicious executable files are run and observed on an isolated computer to determine whether they are indeed viruses. However, this method relies on actual observed program functions and may not be able to reliably detect viruses

that do damage only under specific conditions (e.g., on a specific date and at a designated time). The “heuristic scan” method, on the other hand, uses common patterns to detect specific program structures, yet with this method it is considered more likely that useful programs will be misidentified as viruses.

## Rudra Features – At a Glance

-  Total protection from viruses, worms and other type of malicious software
-  Rudra does not require updates
-  Prevent Unknown and Untrusted programs from running on your computer
-  Rudra keeps track of the files created by various processes and deletes them when created by an un-trusted program
-  Rudra monitors new files creation, changes in system configuration, system control files and in critical application program files for potential threats.
-  Rudra notes all user activity like cut, copy, paste, drag, drop, sendto and rename files or folders
-  Automatic online updates of other software are monitored and only files created by authorized process are considered pre-validated files.
-  Makes Windows Kernel forward all requests for execution to Rudra for

validation. Thereby preventing unauthorized programs from executing.

-  Rudra kills the Malicious Process in the RAM of the computer and deletes the virus file from the hard disk automatically.
-  Rudra's folders protection: Rudra protects its supporting database folders. So any application not related to rudra cannot modify or delete Rudra supporting files.
-  Rudra combats viruses that are capable of self-encryption and polymorphism. Self-encrypting and polymorphic viruses were originally devised to circumvent pattern-matching detection by preventing the virus generating a pattern. Unknown viruses applying this technique are even more difficult to detect.

## Current Operating Systems Support

Rudra currently is available for the following operating systems: Windows 2000/XP