

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

Rudra – “Detecting
UnKnown Computer
Viruses” - A New
Approach



Rudra Technologies Pte. Ltd, Singapore

Company Registration No: 200601277K

www.rudratec.com

RUDRA TECHNOLOGIES PTE LTD- INTRODUCTION

- ❖ Rudra Technologies Pte Ltd, Singapore focuses on Research and Development in inventing new technologies in the software security arena that fulfills existing market needs. Rudra's commitment to continuous innovation has led to a number of technological advances, many of which have set the standards for the whole antivirus industry.
- ❖ The Company has its Global Headquarters in Singapore and fully owned subsidiary in Chennai, India.
- ❖ The Software Product based on its first Revolutionary Technology ("Patent Pending", USPTO under PCT) is fully developed and ready to be marketed globally in the name of "RUDRA".

Rudra protects computers from Past, Present and Future Viruses, Worms, Spy ware, and other Malware by identifying all malicious codes in their UNKNOWN state.

Today's society is more and more dependant on computer networks—in personal communications, corporate activities, and the overall infrastructure. With new viruses emerging every day and spreading with increased rapidity, vigilant defense of computers is essential to the security of the enterprise. 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 signature database and requires no updates. It offers comprehensive protection against viruses, worms, spyware and other malicious software - including those that 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, detecting all viruses in the unknown viruses. Rudra fills this gap with an accurate detection technology that can prevent this damage by and has increased the efforts in pattern extraction to cope with such variants. Since these infections can cause immediate and serious damage, Today, some of the most common sources of virus propagation is through email, 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?



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’s 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



cannot run on your system in order to cause any damage by:

viruses (like signature and heuristic technology). It simply focuses on making sure that the malware.

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 proprietary 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
Virus Signatures	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.

Existing Technology



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

