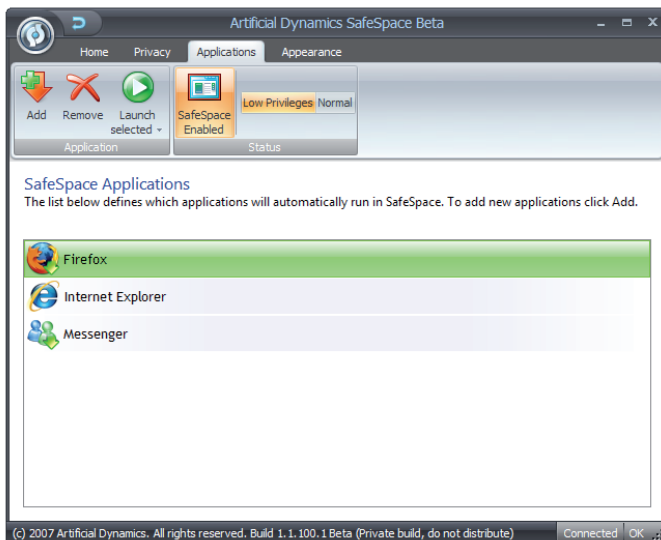




## SafeSpace Corporate Edition

Malware protection is a constant problem to the modern enterprise. Desktop computers, notebooks and terminal servers with access to the internet pose a significant threat to the security of users and the sensitive data they have access to. Even with the latest antivirus, email filtering and perimeter solutions in place, the risk of infection by malware introduced through internet facing applications is increasing.



### benefits

- **Protect against malware such as viruses, spyware, Trojan & root kits**
- **Guard against unknown internet threats**
- **Browse any website in safety**
- **Protect your private data**

### The Problem

Modern malware is being designed to be undetectable. Hackers' motives have evolved because of the lucrative gain to be made through stealing corporate data. Traditional antivirus solutions cannot protect end users from internet threats, and the risk of compromise through an endpoint with internet access is growing exponentially, with no sign of stopping.

This risk is not limited to just web browsers. Instant messaging clients are fast becoming a key communication method across distributed offices, and are also being targeted by hackers. Documents downloaded from the internet can also pose a danger to end users, because of the ease with which code embedded in popular formats can bypass perimeter and endpoint scans.

The legal ramifications of leaked sensitive information, loss of competitive edge and loss of customer confidence can be catastrophic to corporate reputation, not to mention the disruption caused by data corruption, downtime and further network exploits.

## The SafeSpace Solution

SafeSpace provides an alternative approach to internet security. By sandboxing internet applications in a secure, virtual environment, a secure barrier is created which protects desktops, notebooks and terminal servers from both known and unknown malware threats. If an internet application or a downloaded file is infected with an exploit, the effects are contained within the SafeSpace environment. When the user next logs off, the virtual environment is destroyed, and so is the malware, leaving the endpoint completely clean from infection.

SafeSpace does not require signatures, heuristic analysis, or any other rules to work. It is always up to date. It stops malware from infecting endpoints, and stops spyware from accessing private files.

SafeSpace is a seamless, secure barrier between the enterprise and the dangers of internet.

## system requirements

### Hardware

- PC with 400Mhz Processor, or higher
- 128 Megabytes RAM, or higher
- 10 Megabytes disk space (Installation)
- Up to 200 Megabytes disk space (Usage)

### Software

- Microsoft Windows XP with Service Pack 2 (32-Bit Edition) or
- Microsoft Windows Vista (32-Bit Edition)
- Microsoft Windows Installer 3.1, or greater
- Microsoft .Net Framework Version 2.0 (XP only)
- Microsoft Core XML Services 6.0 (XP only)