

Sanctuary[®] Feature Matrix

Feature/Benefit	Sanctuary [®] Citrix Solutions		
	Presentation Server	Access Gateway	Access Devices
Central Policy Enforcement	✓	✓✓✓	✓✓✓
Enhanced Security	✓	✓✓✓	✓✓✓
Improved Availability	✓	NA	NA
Prevent Malware execution (Spyware, etc.)	✓	NA	✓✓
Authenticated Execution	✓	NA	✓✓
Patch On Your Schedule	✓	NA	✓✓
Reduce Data Leakage	✓	NA	✓✓✓
Prevent unauthorized and unlicensed software from executing	✓	NA	✓✓
Comprehensive Auditing	✓	NA	✓✓✓
Microsoft XPe Support	NA	NA	✓✓✓
Prevent usage of unwanted or non corporate devices	NA	NA	✓

Sanctuary Product Solutions include:

- ✓ SACT = Sanctuary Terminal Services Edition
- ✓ SACCE = Sanctuary Custom Edition
- ✓ SDC = Sanctuary Device Control

To see how Sanctuary can reduce your Citrix environment's TCO request an evaluation:

www.securewave.com/evaluation

Sanctuary[®] Feature Definitions

Features/Benefits	Definitions
Central Policy Enforcement	Sanctuary provides a definitive way to enforce policies throughout any organization at both device usage and application access/execution level based on a white list principle: if the user / remote user does not have access to a specific device or application, device or application access is stopped at kernel level.
Enhanced Security	Enforcing policies is combined with reduced risks of intrusions at both access device levels and presentation server. Data theft, illegal information access, illegal software execution or unwanted plug-and-play device connections are under control with Sanctuary.
Improved Availability	By controlling at kernel level what code can execute on a Presentation server, Sanctuary reduces the risks of disruption and unavailability of a critical business application to the organization. No malware will ever be able to execute, giving back the total control of the environment to the system administrators.
Prevent Malware execution	As only authorized code can run, Sanctuary is protecting by default against ALL known or unknown malware, including spyware, viruses, Trojans, software keyloggers, rootkits, hacking software, etc. and this from the beginning: no need to wait for AV subscription services updates.
Authenticated Execution	Prior to allowing a program to execute, Sanctuary will authenticate the code using the well-known SHA-1 algorithm. Only authorized code are allowed to run, hence making sure only legitimate applications are accessed by authorized users/remote users.
Patch On Your Schedule	Eliminates the need to rush the implementation of patch due to a critical security alert. Only authorized process are allowed to run.
Reduce Data Leakage	Granular control of application execution and removable devices (USB, FireWire, etc.) eliminates, even an authorized user from copying sensitive files from the network to a storage device (e.g. PDA, iPod, memory sticks, external hard drives, etc.).
Prevent unauthorized and unlicensed software from executing	As only authorized code can run, Sanctuary is protecting by default against illegal, unwanted applications as well as known and unknown malware, including spyware, viruses, Trojans, software keyloggers, rootkits, hacking software, etc.
Comprehensive Auditing	Sanctuary Device Control is able to shadow all data copied to external devices or specific ports (file names only or full copy of files transferred). Full auditing of all Administrator actions is also available throughout Sanctuary products and advanced reporting is available on both devices and applications access attempts.
Microsoft XPe Support	In addition to Windows 2000, Windows 2003 and Windows XP support, Sanctuary also supports Windows XPe in order to provide organizations the way to achieve their TCO goals by using thin clients access devices instead of regular PC workstations.
Prevent usage of unwanted or non corporate devices	Sanctuary controls access to devices by applying a device Access Control List (ACL) to users, user groups and even specific computers. No device access is possible if not centrally authorized for the user/remote user.