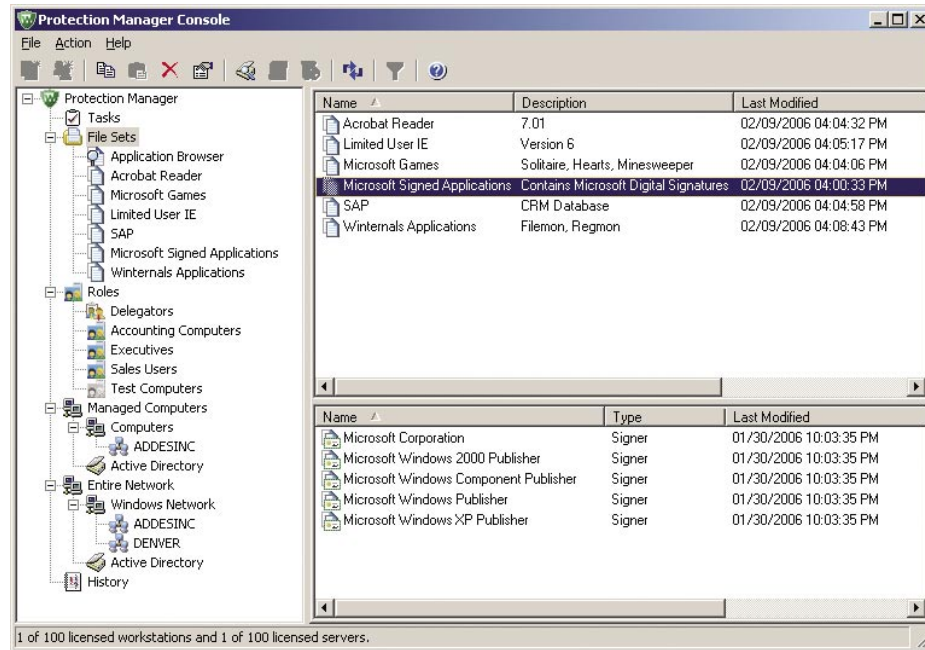


# Protect Windows Systems *throughout your enterprise.*

**Winternals Protection Manager stops unauthorized applications from executing and enables successful least privilege.**



Protection Manager™ creates a least privilege environment where users have only the power required to do their jobs efficiently, while prohibiting the execution of applications you have not specifically authorized to run in your environment.

When you roll out Protection Manager, you go through a series of deployment modes that gather information and ease the transition for end users. You use a simple wizard to create Roles, then add Members and applications (called File Sets) to them. You control the way Members of a Role execute applications in one of four ways (allowed to execute, execute with administrative privileges when required, execute with limited user privileges, or denied from executing under any conditions).

Administrators have the ability to delegate the approval of applications within IT, recognizing the fact that a decentralized approach allows organizations to allocate approval rights more effectively. Delegation is also the key to scalability, making Protection Manager the right solution for any size enterprise.

Protection Manager prevents unauthorized executables from running in your network, providing you with protection from both zero-day attacks and violation of regulatory and software license compliance.

## The Protection Manager Advantage

### STOPS MALWARE IN ITS TRACKS

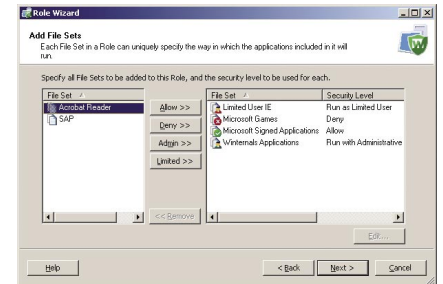
Protection Manager closes the 'window of vulnerability' that exists during the time after malware is released and before other security solutions can be updated.

### PREVENTS ACCIDENTAL DAMAGE BY USERS

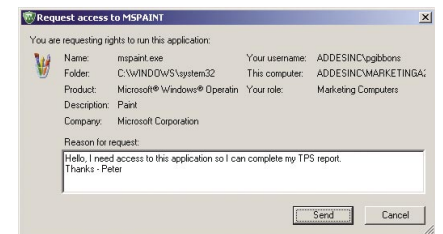
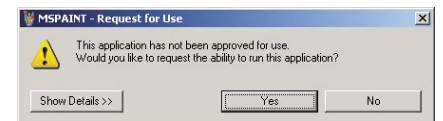
Protection Manager allows users to run necessary applications at elevated levels of privilege while maintaining their status as users in every other context.

### KEEPS USERS PRODUCTIVE

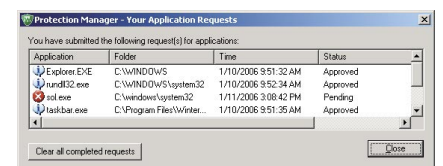
Protection Manager is designed to minimize the impact on end users while maximizing the security and stability of their systems.



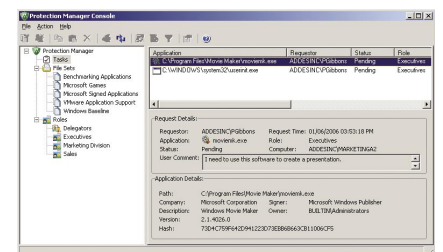
Easily add one or more File Sets to Roles with Administrator-defined security privileges.



Users who need access to new applications can request permission to run them.









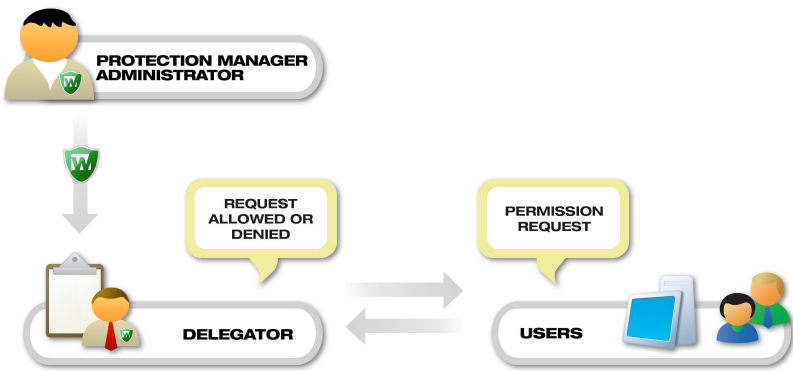
Users can view a list of their application requests and the request status.



Delegators respond to application requests and either allow or deny access to the applications real time.

*"Moving all of my end users out of the 'Administrators' group is a security no-brainer. But with legacy apps that need admin rights and a stack of productivity obstacles it simply wasn't feasible. With Protection Manager, we can do it, and it works. This product gives the control back to the administrator on a whole new level."* – Robert Guidarini • IT Manager, Clear Channel Communications

*“...anti-malware investments should be your highest priorities, because these offer the greatest potential for TCO reductions.”* – Gartner • Security Best Practices Can Lower PC TCO<sup>1</sup>

FEATURES AND CAPABILITIES		REQUIREMENTS
<b>Application Browser™</b> Displays and filters all applications captured from protected systems for easy set up of File Sets.		<b>CONSOLE REQUIREMENTS</b> The Protection Manager Console requires the following minimum system configuration: <b>Platform:</b> 900 MHz or higher Intel® Pentium® compatible CPU <b>Active Directory:</b> Console system must be an Active Directory member <b>Memory:</b> 256MB RAM <b>Network Adapter:</b> 10 megabit or faster wired Ethernet adapter <b>Available Hard Disk Space:</b> 100MB required for the Protection Manager Console <b>Operating System:</b> Microsoft Windows 2000 SP4, Windows Server 2000 SP4, Windows XP Professional SP2, Windows Server 2003 SP1
<b>File Set Security</b> Designates applications as: allowed to run, run with administrative privileges when required, run with limited user privileges, or denied from running under any conditions.		
<b>SmartStop™</b> Monitors the creation of all processes on a system, intercepting denied applications before they can run.		
<b>SmartRun™</b> Permits applications to run in the user's security context but with increased privileges in order to accommodate applications which require administrative privileges to run – without the user being a member of the Administrators group.		
<b>Run Time Permission Requests</b> Allows users to instantly request access to unknown applications, making enforcement of your 'acceptable use' policies possible in a way that won't interfere with productivity.		
<b>Deployment Modes</b> Provides an introductory stage that lets administrators gather application data and define permissions, while easing transition to the new policies for end users.		<b>CLIENT REQUIREMENTS</b> The Protection Manager client requires the following minimum system configuration: <b>Platform:</b> 233 MHz or higher Intel Pentium compatible CPU <b>Active Directory:</b> Client systems must be Active Directory members <b>Memory:</b> 128MB RAM <b>Network Adapter:</b> 10 megabit or faster wired Ethernet adapter <b>Available Hard Disk Space:</b> 10MB required for the Protection Manager Client <b>Operating System:</b> Microsoft Windows 2000 SP4, Windows Server 2000 SP4, Windows XP Professional SP2, Windows Server 2003 SP1
DELEGATION		
 <p>Administrators can create Delegators and assign Roles to them to manage. This allows administrators to manage a large network while assigning Protection Manager tasks to Delegators who are familiar with their users' needs.</p>		

**Microsoft®**  
**GOLD CERTIFIED**  
Partner

**Winternals®**

3101 Bee Caves Road

Suite 150

Austin, TX 78746

www.winternals.com

Ph 512.330.9130

Fax 512.330.9131

<sup>1</sup> Gartner Research, "Security Best Practices Can Lower PC TCO", Michael A. Silver, Neil MacDonald, Mark Nicolett, and John Pescatore, 8 December 2005.