



Keep unwanted **software** from **running** with



Patent-pending technology immediately denies access to any program or file, on any desktop—even if it's already open.

These days, there's a plethora of software that can wreak havoc on your enterprise:

- Viruses and worms that can bring down the network,
- File sharing programs and spyware that open holes in the firewall,
- Unmonitored instant messaging,
- Illegal music and movie players,
- Applications that violate corporate desktop standards, and more.

The negative impact of these programs is extensive, ranging from elevated operational costs, legal exposure, and security risks, to reduced productivity or even complete crippling of the business.

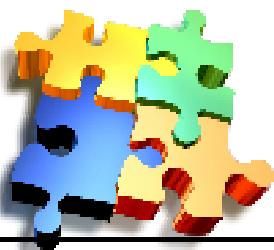
OverSight utilizes Tangram's proprietary technology to stop these programs, as well as any other specified computer file, from running in your enterprise—ever.

This powerful new solution allows you to deploy policies that deny access to any given file or application, at any level.

If a user attempts to copy it, rename it, or otherwise alter it, OverSight won't allow it. If a file is already running on a targeted desktop, OverSight instantly kills it, wiping it from memory.

OverSight™ offers powerful new options for taking control of your enterprise.

And, OverSight gives you highly granular control over which desktops are subject to a given policy, by geography, business unit, individual desktops, or the entire enterprise. Whether you're responsible for help desk support, software license management and compliance, or corporate security, OverSight offers exciting new options for taking control of your enterprise.



OverSight allows you to create customized messages (above) that will appear when anyone attempts to open an undesirable file or application on their desktop.



The Policy Management Console allows you to define, select, and distribute "policies," or rules, and then monitor their progress.



The Technology behind the Solution

OverSight runs in conjunction with either Asset Insight® or the unified Insight solution, Tangram's IT asset management software. To block access to a particular file or program, the organization's designated manager goes to the Policy Management Console (see graphic) and selects a predefined "policy" (rule) or defines a new policy, which includes control options over execution, rename, copy, delete, and read access. The manager then identifies the target computers, and creates customizable end-user and system messages. Finally, the manager pushes the policies to the enterprise with a click of a button and monitors the progress of distribution. Policies are sent out to the appropriate desktops, either immediately or on schedule, via Asset Insight's software distribution methodology, where OverSight's Compliance Monitor uses the patent-pending technology to monitor for and deny access to any file defined in the policies. If the undesirable file or application is already open on the desktop, it will disappear and the administrator's message will pop up (see sample message graphic). Other features include:

- Warm and Hot Locks—Hot Locks are for policies that require immediate distribution, such as viruses and other security threats. A Warm Lock is used when speed is less of a prerequisite (e.g., with desktop standards

enforcement), and policies are sent out via Asset Insight's normal distribution schedule.

- Illegal Policy Screener—Predefined policy screens help to prevent erroneous or malicious policy creation.
- OverSight Reports and Guru—The OverSight manager has extensive reporting capabilities to both select the target desktops, and later see which desktops attempted to access undesirable files or programs.
- OverSight ships with a number of predefined reports, as well as ad hoc reporting functionality. The Guru's drilldown options allow you to check the status of problem desktops.

OverSight users also have the advantages of Asset Insight for best-of-breed auto-discovery and tracking of hardware, software, configuration files, and software usage, from mainframes to PDAs, scalable across even the largest enterprise. Additionally, organizations with OverSight and the unified Insight solution combine auto-discovery and access control with a repository of financial and contractual data for comprehensive IT asset management.

To find out how OverSight can benefit your organization, please call +61 29409 1000 or visit www.resonancegroup.com.

The Resonance Group Pty Ltd
 ABN 22 097 035 893
Resonance Australia
Head Office
 100 Walker Street
 North Sydney NSW 2060
 Telephone 61 2 9409 1000
 Facsimile 61 2 9409 1010

