

VMBlocker™

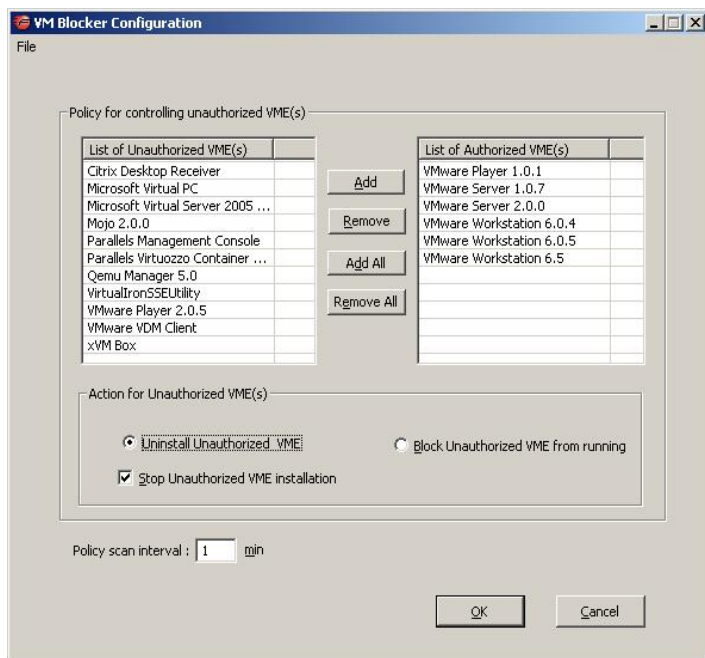
RedCannon VMBlocker is one of the most powerful end-point enforcement solutions available to organizations for ensuring Virtualization compliance in their network by restricting all VM environments on each computer to only the authorized ones approved by the Enterprise. Using a patent-pending technology it can identify & enforce Enterprise policy on all known Type-2 VM Environments.

With abundant availability of free Virtualization products such as VMWare Server, WorkStation, Player, Microsoft Virtual PC and Sun xVM Virtual box, organizations are rushing to adapt this new, exciting & efficient technology. However unplanned and unauthorized Virtualization platforms cause as much IT and Security related issues as unauthorized physical computers. Deployment of Virtualization in any Enterprise organization should be controlled & policy-driven roll-out like any other Computer platform, software or application.

RedCannon VME Blocker: RedCannon VMBlocker is an end-point security software that resides on each computer where none or only a specific Virtual Machine Environment (VME) is allowed. Through centrally configured policy & a simple software deployment process such as Windows group policies, each computer on the Enterprise network can be immediately made compliant by removing any unauthorized VMs & VMEs from those computers & blocking any future installations.

Detect & Remove Unauthorized VMs : Unauthorized VMs could pose more security risk than unauthorized physical machines because of a) physical machines can be detected through NAC & b) VMs can be created & deployed very easily and within minutes. With freely available virtualization platforms that run on standard Windows desktops, any user with local privilege can install & create number of VMs which can be used without any Enterprise detection.

Conventional Network Access Control (NAC) solutions won't typically control unauthorized VMs since these VMs could use NAT to eliminate risk of detection by leveraging authorized IP Address of the Host machine.



Protect Type-1s, Restrict Type-2s: VMEs aka Hypervisors are available in two different modes. Type-1 hypervisors work “bare metal” i.e. directly on top of the physical hardware of the computer while Type-2 hypervisors run as a process within another Host OS. Majority of the freely available hypervisors are of Type-2. It's critical for the Enterprise to restrict usage of these VMEs since they are the easiest to acquire & deploy without IT knowledge.

Secure VDI Deployments: Virtual Desktop Infrastructure or VDI has steadily gained ground because of the ease of deployment, management & patching of virtual desktops. Enterprises need to ensure that VDI components deployed on each physical desktop would only allow their specific VDI to run & no other VM environments. This helps eliminate any potential vulnerabilities introduced by any other VME on Enterprise desktops.

Eliminate Compliance Risks & Security Exposure: Enterprises spend painstakingly long time & resources to ensure and enforce Network & Computer security for every asset owned by the Enterprise. From a compliance & security risks perspective, the threat of unauthorized VMEs is far greater than an unauthorized physical computer. Therefore just like physical computers, enterprises need to enforce strict compliance on usage of such VMEs.

Utilizing its patent-pending technology VME Blocker identifies & enforces compliance by blocking or removing unauthorized Type-2 VMEs from Enterprise PCs.

Features:

- Eliminate
 - Unauthorized VMEs
 - VM Vulnerabilities and security risks
 - Secure VDI deployments (VMWare or Citrix)
 - VM Data Leakage
- Automatically detects & removes/uninstalls any unauthorized Type-2 Hypervisors from any Windows computer
- Auto-detects installation of an authorized VME & immediately stops the installation process
- Supports most Windows-based VMEs with Type-2 Hypervisor
 - VMWare Server, WorkStation, Player & VDM Client
 - Microsoft Virtual PC & Virtual Server 2005
 - Sun xVM Virtual Box & Citrix XenDesktop Client
 - others
- Centrally configurable policy & Silent install for central deployment
- Patent-pending Technology

Specifications:

- Works on Windows Vista, XP SP2, Windows 2000 & Windows 2003 Server
- Deployed using standard Windows software distribution methods such as Group Policies