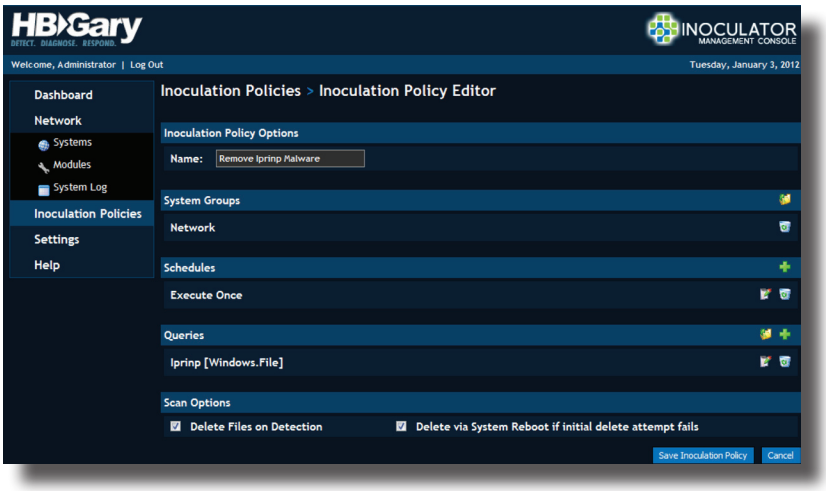
INOCULATOR

Inoculator™ conducts fast, agentless scans for known APT and other targeted threats



Stop Waiting. Start Protecting.

HBGary Inoculator™ detects, removes and prevents Windows® host re-infection of known Advanced Persistent Threats (APT) and other targeted threats for the enterprise. You can't afford to wait days, weeks or months for your antivirus vendor to provide a detection signature to protect your company's most important assets.

Active Defense™ Integration

With HBGary's flagship product, Active Defense™ with Digital DNA, organizations can monitor host physical memory, raw disk, and live operating systems concurrently across the enterprise to get an unprecedented view of host-level, new and unknown threats. Together, HBGary Inoculator™ and Active Defense™ with Digital DNA provide the first enterprise solution to detect and remove both known and unknown APT and other advanced cyber threats.

Automated Network Scans

Inoculator™ can remotely and automatically scan the enterprise for the most advanced, state-sponsored threats today, out of the box, with no additional supplied user data besides domain credentials. If a machine gets re-infected with an artifact of APT or malware, or if that APT artifact shows up somewhere else in the enterprise, Inoculator will detect the recurrence and alert the user.

Inoculator Features

Default Scan – Inoculator™ automatically detects malicious remote administration tools that give attackers unrestricted access to your data.

Agentless Management – Inoculator™ interfaces with your Microsoft Active Directory server, and communicates with systems using only remote procedure calls, resulting in zero performance impact to the end node.

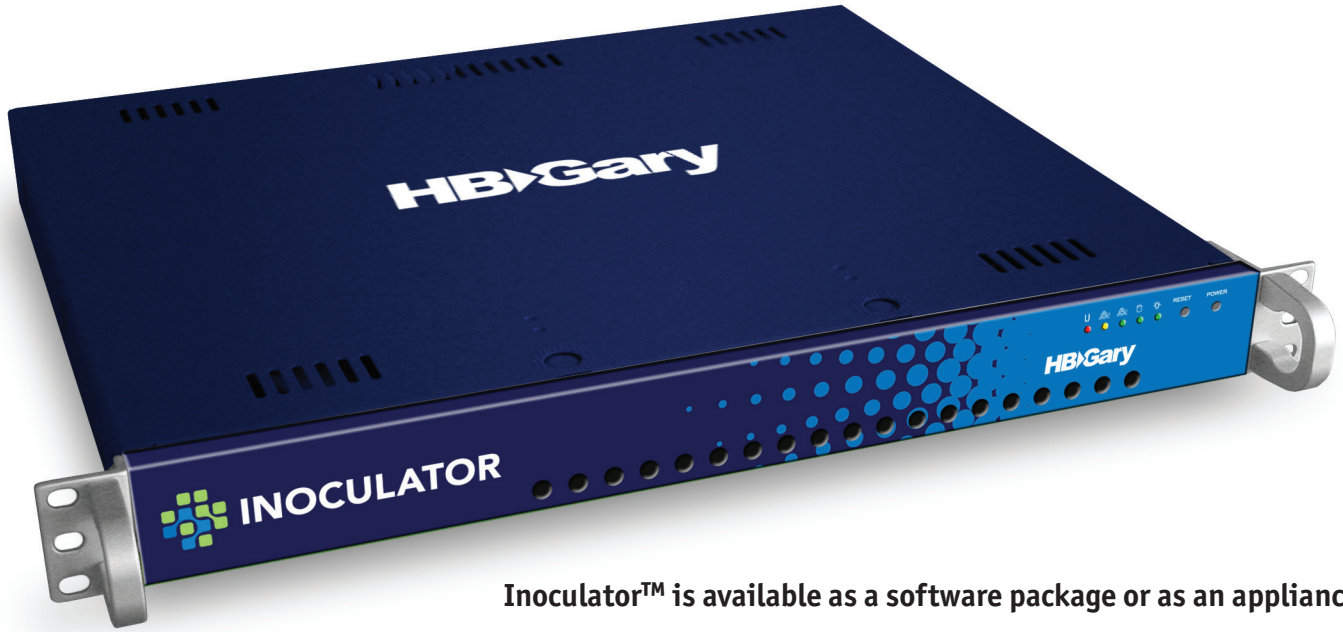
- Inoculator™ detects and removes malware and other APT components and artifacts on the fly without agents.
- End nodes are managed using a group interface.

Inoculator Policies – Allows organizations to perform user-defined searches for specific bad files and registry keys that malware uses to persist on a system.

- Once detected, malware can be automatically deleted on systems, and a centralized alert is logged.

HBGary
Detecting Tomorrow's Threats Today
3604 FAIR OAKS BLVD, SUITE 250 | SACRAMENTO, CA 95864 | PHONE: 916-459-4727 | WWW.HBGARY.COM

Inoculator™ puts threat remediation into your hands



Inoculator™ is available as a software package or as an appliance.

System Requirements

The Inoculator™ software is installed on a server, which may or may not contain storage for a database. The Inoculator™ server is a computer running the Inoculator software package, which provides the user interface and remote node management features.

The Inoculator™ server must meet the following minimum system requirements:

- System Administrator access for installing applications .
- Microsoft Windows Server 2000® (with Service Pack 4+), Microsoft Windows XP® (with Service Pack 2+), Microsoft Windows 2003®/2008®/Vista®, Microsoft Windows 7® 32- and 64-bit.
- Minimum 512MB of RAM. (The minimum amount of RAM recommended for your specific operating system is sufficient for the Inoculator server. For example, Windows Server 2008® recommends 2GB of RAM for the OS.)
- Minimum 10MB of available hard disk drive space for the Inoculator™ server management application.
- Minimum 20GB of hard disk drive space recommended for the Inoculator™ database.

The following prerequisite packages are located on the Inoculator™ CD:

- Microsoft .NET framework version 3.5
- Microsoft SQL (MSSQL) Express 2008

Supported Operating Systems

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7

HBGary
Detecting Tomorrow's Threats Today
3604 FAIR OAKS BLVD, SUITE 250 | SACRAMENTO, CA 95864 | PHONE: 916-459-4727 | WWW.HBGARY.COM