



Technology Today
for the Threats
Tomorrow



3232 LeBlanc
San Antonio, TX 78247
Phone: (210) 490-4018
Fax: (210) 490-0494
www.threatguard.com

TM: A Registered Mark of NIST, which does not imply product endorsement by NIST or the U.S. Government

Secutor Magnus

Datasheet

OVERVIEW

Secutor Magnus is the first product designed specifically to meet the Common Security Configurations requirements set forth by the Federal Government's Office of Management and Budget (OMB). Built for the "Information Security Automation Program" (ISAP) as established by the National Institute of Standards and Technology (NIST), Magnus fully supports a wide-scale action plan to quickly and continually show that an organization has compliance under control. The entire Secutor line of automated content tools provides standardized assessments, content-driven remediation, and complete mappings to driving requirements with options to easily document deviations from those requirements. With over 2000 evaluators from government, military, commercial, and academic locations, Secutor provides operational confidence to network administrators, system integrators, and IT service providers. NIST has ushered in a new era of standards-based compliance assessment. Secutor Magnus meets those standards to the fullest, and extends them to be a complete compliance solution.

Key Features:

Test NIST configurations to identify adverse effects on system functionality

- * Desktop module places a system in 100% compliance in under 60 seconds.
- * Selective undo/redo/restore supports quick adjustments to test effects.
- * System profiler exports deviations for operational assessments and remediation.

Automated enforcement

- * Magnus scheduler periodically assesses compliance across the network.
- * Notifications alert specified personnel when systems fall out of compliance.
- * Optional setting to reapply remediation on detection of altered systems.

Restrict administration to authorized professionals

- * Magnus requires proper credentials to view and apply settings.
- * Executive-level views permit read-only access to compliance status.

Ensure new acquisitions use standard configurations

- * Desktop module can enforce standards prior to deployment of new systems.
- * Operational profiles apply authorized deviations during lockdown procedures.

Patches

- * Automatically determines if computers have all required security patches.
- * Performs vulnerability assessment of operating system and major applications.

Provide documentation of deviations with rationale

- * System profiler enables simple, yet full-featured deviation system, including accountability, documentation, expiration, traceability to requirements, and recognition during assessments and remediation.

Architecture and supported platforms

- * Windows XP, Window Vista, Windows Server 2003 – more platforms will be added as NIST releases content including Solaris and Red Hat Linux.
- * Requires Microsoft .NET 2.0 or greater (included)