Belarc's product mapping to NIST 800-53 rev 4 controls
15-Jul-12

Belarc's products monitor many of the technical controls in the NIST document referenced above. In addition Belarc's system can help in the assessment of some of the non-technical controls to help determine if they are effective for the organization. Because Belarc's data is automatically gathered once per day and stored in a central repository, there is no need to spend time and effort on data calls. Rather the IT security staff can spend their efforts in making proper decisions based on accurate and up-to-date information in their exiting repository. See the information on Belarc's system architecture for details. Also, see our white paper, "Securing the Enterprise" for a more detailed discussion on these topics.

Control No., Control Name, Assurance, Control Baselines (low, mod, high)	How BelManage or BelSecure can help achieve this control	Example Screenshots
AC-2 Account Management x x x	Belarc helps with "Reviewing accounts for compliance with account management requirements", identifying users with administrative privileges, and the status on local and domain accounts, i.e. locked accounts, disabled accounts, accounts with passwords older than 90 days, and accounts with unusual privileges.	http://www.belarc.com/Archive/local_user_accounts.jpg
AC-2 (1) ACCOUNT MANAGEMENT | AUTOMATED SYSTEM ACCOUNT Management xx	Belarc is an automated system.	http://www.belarc.com/Archive/Domain_accounts.jpg
AC-2 (3) ACCOUNT MANAGEMENT | DISABLE INACTIVE ACCOUNTS x x	Belarc automatically discovers inactive accounts with last logon time, including accounts that have never logged on.	
AC-2 (4) ACCOUNT MANAGEMENT | AUTOMATED AUDIT ACTIONS x x	Belarc automatically audits new accounts, modifications, etc.	
AC-2 (12) ACCOUNT MANAGEMENT | USAGE CONDITIONS x	Belarc automatically audits account usage across different computers.	
AC-2 (13) ACCOUNT MANAGEMENT | ACCOUNT REVIEWS x	Belarc automatically gathers the required data for these account reviews, such as access authorizations and shared and group accounts.	
AC-2 (14) ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE	Belarc monitors for atypical usage, such as accounts logging on to multiple machines.	
AC-2 (15) ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK Individuals	Belarc audits account logon activity of all users, including high risk users.	
AC-18 Wireless Access x x x	Wireless technologies include, for example, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. BelManage automatically discovers all network connected devices, including wireless routers, and host devices such as Bluetooth.	http://www.belarc.com/Archive/host_devices.jpg
AC-18 (2) WIRELESS ACCESS | MONITORING UNAUTHORIZED CONNECTIONS W Incorporated into AC-18.	See above.	http://www.belarc.com/Archive/network_attached_devices.jpg

Control No., Control Name, Assurance, Control Baselines (low, mod, high)	How BelManage or BelSecure can help achieve this control	Example Screenshots
AC-19 Access Control for Mobile Devices x x x	From the NIST guidance: "Mobile devices include portable computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Belarc's products automatically gather the configuration data on notebooks, even when they are not connected to the network. The next time that they logon to the network, via VPN for example, their profile data is automatically uploaded to the BelManage server.	
	Belarc's products will also detect PDAs, cell phones, digital cameras, iPods, etc. when they connect to a host device. BelManage detects these devices, their usage history, whether they are approved devices and who authorized their use on the network. See the sample screenshot.	http://www.belarc.com/Archive/storage_device_use.jpg
AC-19 (6) ACCESS CONTROL FOR MOBILE DEVICES | FULL DISK ENCRYPTION x x	BelManage automatically discovers disk encryption, state and type.	http://www.belarc.com/Archive/disk_encryption.jpg
AU-2 AUDITABLE EVENTS	Some or all of the BelManage configuration data may be useful as forensic data in an auditable event. In particular the anti-virus status, user logon data, IAVA or security update status, software and version data.	
AU-8 TIME STAMPS	The BelManage data is time stamped using GMT.	
CA-7 Continuous Monitoring A x x x	From the NIST guidance:"...Having access to security-related information on demand gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely."	
	Belarc's products automatically gather the software, hardware and security configuration data of the systems' hosts and network attached devices on a continuous basis, usually daily. This configuration data is automatically uploaded to a central repository that is used to create web based reports, or for direct access via ODBC connections or SQL queries.	

Control No., Control Name, Assurance, Control Baselines (low, mod, high)	How BelManage or BelSecure can help achieve this control	Example Screenshots
	Because this configuration data is always up to date, it allows the IT security and management personnel to make better and more timely risk management decisions based on accurate, current and complete configuration data. In addition Belarc's products support the SCAP standards, such as CPE (Common Platform Enumeration) and ARF (Asset Reporting Format), which will help make the Belarc data easily used by other systems also using these SCAP standards.	
CM-2 Baseline Configuration A x x x	BelManage automatically gathers the configuration data specified in the NIST guidance including, "Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters),..."	
CM-2 (1) BASELINE CONFIGURATION | REVIEWS AND UPDATES A x x	BelManage automatically updates the configurations based on actual current data. In addition BelManage can compare the current accurate configurations to standard configuration images.	
CM-2 (2) BASELINE CONFIGURATION | AUTOMATION SUPPORT FOR ACCURACY/Currency A x	See above.	
CM-2 (3) BASELINE CONFIGURATION | RETENTION OF PREVIOUS Configurations A xx	BelManage's Change History module automatically retains all of the software, hardware and security configuration adds and removes of all of the monitored host devices, including laptops, desktops, servers.	
CM-2 (4) BASELINE CONFIGURATION | UNAUTHORIZED SOFTWARE W Incorporated into CM-7.	See CM-7	
CM-2 (5) BASELINE CONFIGURATION | AUTHORIZED SOFTWARE W Incorporated into CM-7.	See CM-7	
CM-2 (6) BASELINE CONFIGURATION | DEVELOPMENT AND TEST Environments A x	BelManage allows for configuration data from unconnected network, such as test environments or secure environment to be uploaded to the BelManage server.	
CM-3 Configuration Change Control A x x	BelManage's Change History module automatically documents all of the adds and removes to the software, hardware and security configurations on the host devices. This data can then be compared to the authorized changes to determine any anomalies.	http://www.belarc.com/Archive/change_history.jpg
CM-3 (1) CONFIGURATION CHANGE CONTROL | AUTOMATED DOCUMENT /NOTIFICATION / PROHIBITION OF CHANGES A x	BelManage audits all relevant changes to the information system and allows for automated comparisons to accepted baselines.	
CM-3 (3) CONFIGURATION CHANGE CONTROL | AUTOMATED CHANGE IMPLEMENTATION	See above.	

Control No., Control Name, Assurance, Control Baselines (low, mod, high)	How BelManage or BelSecure can help achieve this control	Example Screenshots
CM-6 CONFIGURATION SETTINGS	BelSecure automatically compares the hosts' configurations to the FDCC and USGCB configuration benchmarks.	http://www.belarc.com/Archive/fdcc_usgcb.jpg
CM-8 Information System Component Inventory A x x x	BelManage meets all of the NIST guidance for system component inventory. From the NIST guidance: "Information deemed necessary for effective property accountability includes, for example, hardware inventory specifications, software license information, software version numbers, information system/component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location."	http://www.belarc.com/Archive/individual_profile.jpg
CM-8 (1) INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS A x x	BelManage automatically updates the system inventory data on a daily basis and enters the data into a central repository. In addition BelManage automatically discovers Virtual machines and their relationship to hosts they're running on.	http://www.belarc.com/Archive/virtual_machines.jpg
CM-8 (2) INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE A x	BelManage automatically updates the configuration data including that for virtual machines, a concern specified in the NIST guidance.	
CM-8 (3) INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION A x	BelManage automatically detects all network attached devices. If any of those host devices, which may be unauthorized devices and do not have a BelManage client installed, the system is automatically notified.	http://www.belarc.com/Archive/systems_without_client.jpg
CM-8 (4) INFORMATION SYSTEM COMPONENT INVENTORY | PROPERTY ACCOUNTABILITY INFORMATION A x	BelManage allows ownership or authorization to be assigned to host devices.	
CM-8 (5) INFORMATION SYSTEM COMPONENT INVENTORY | ALL COMPONENTS WITHIN AUTHORIZATION BOUNDARY A x x	BelManage automatically discovers all of the devices connected to the network, and also identified any of the host devices that do not have a BelManage client installed. These devices may be unauthorized devices.	
CM-10 Software Usage Restrictions x x x	BelManage automates software license tracking and software usage to help optimize software license management. The NIST guidance is mostly concerned about the use of software over the authorized license amounts. However many organizations are spending more on software licensing and annual maintenance than necessary. BelManage also helps to optimize these annual costs to the organization.	http://www.belarc.com/Archive/software_licenses.jpg
CM-11 User-Installed Software x x x	BelManage automatically discovers all of the installed software and versions on the host devices. Reports can be created to automatically compare the installed software and versions to approved software or explicit version ranges.	http://www.belarc.com/Archive/noncompliant_software.jpg
CM-11 (1) USER-INSTALLED SOFTWARE | AUTOMATED ALERTS FOR UNAUTHORIZED INSTALLATIONS	BelManage allows for automatic alerts on the installation of unauthorized software.	

Control No., Control Name, Assurance, Control Baselines (low, mod, high)	How BelManage or BelSecure can help achieve this control	Example Screenshots
CP-7 (4) Alternate Processing Site | Configuration For Use	BelManage audits the configuration of an alternate processing site, continually showing its readiness for operation and correct configuration. Any changes to the alternate site configuration are show in change history reports.	
RA-5 (7) VULNERABILITY SCANNING | AUTOMATED DETECTION AND NOTIFICATION OF UNAUTHORIZED COMPONENTS	BelManage can automatically notify of unauthorized software and unauthorized devices on network.	

For additional information please contact us:
Belarc Benelux
(ITAMSoft B.V.)
Den Ilp 8
1127PA DEN ILP (Amsterdam)
Tel: +31 (0)20 - 4822603
Email: info@belarc.nl
Web: http://www.belarc.nl