Global Information Assurance Certification Paper

A primer for PC secured configuration compliance monitoring solution

Efi Kaufman

September 2004

GIAC Security Essentials Certification (GSEC)
Version 1.4b Option 1

Abstract:

Monitoring the configuration of computing systems is known as one of the major phases in a security management process. While the compliance monitoring component is most often integrated within a product or a security suite, the bigger the number and variety of computing systems in an organization, the bigger the chance that a component designed specifically for the task of compliance monitoring will need to be purchased or developed.

This paper describe the most important features and guidelines for planning, developing and choosing a compliance monitoring solution whether it is a stand-alone application or a component within a security management suite, bought from a vendor or in-house developed.

1. The security baseline

A security policy is a document that describes what must be done in order to protect people and information. The security policy on one hand set the usage standards for systems users and on the other hand set the guidelines for the security personnel in charge of keeping these standards.[1]

Security policies can be based on both company-specific requirements and industry-standard regulations. Important recent examples of industry-standard privacy and security regulations include[2]:

- Sarbanes-Oxley
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Federal Trade Commission Information Safeguards Regulations

As part of the security policy, issue specific policies that refer to systems configuration must also be defined. This includes[3,4]:

- System access control – describing password best practice, desired security settings for services, files, registry access and other local security settings.
- Host based safeguards - applications like Antivirus and personal firewalls.
- Software installations – describing the licensing model for allowed applications and guidelines for unauthorized software including spyware, adware and other non-legitimate software.
- Security patches level – describing the desired status of the systems with regard to the installations of security related patches and service packs.

In order to cover these issue-specific items and the dynamic security related configuration items in the security policy, the security policy will refer to a *security baseline* or *a secured configuration* which will be defined separately from the security policy and will change as new patches and configuration changes will be applied to the different platform in order to make them secured.

Security-baseline is defined and referred to as a set of configurations and

access controls that affect the overall security state of the computer system and the information stored on it.

2. Compliance monitoring defined

The term *compliance monitoring* in the context of PC security is also known as *compliance scanning*, *policy management*, *policy compliance*, *configuration management* and more. The formal definition of compliance monitoring is the following:

"Detect and track policy violations and other security vulnerabilities to help ensure that resources facilitate the resolution of security issues"[5]

The compliance monitoring in this case is done on endpoints that should be part of an organization asset and therefore should have the permission to access them or to install an agent, as opposed to vulnerability scanner which does not assume an access to the endpoint exists but rather make use of the vulnerability itself to report if a platform is vulnerable or not.

3. The Role of the compliance monitoring system

Once the secured baseline configuration is defined , it is expected from a compliance monitoring application to constantly monitor and check the systems compliance with the defined secured baseline.
it might check for the following:

- Status of security patches deployment.
- The presence and running status of Host Intrusion Detection Systems (HIDS).
- The presence of Anti-Virus application and up-to-date signature files.
- Status of malware installations or applications which are not allowed to be installed

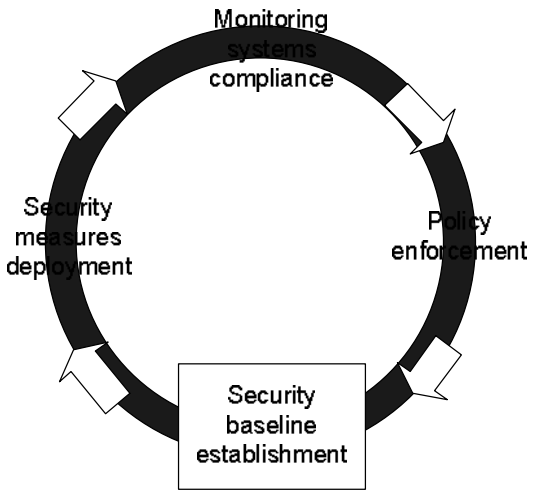

Image 1: Compliance monitoring role in a security management process

Naming the above, one might rightfully ask why this is needed when most of the applications meant to secure a PC system have their own backend infrastructure to make sure the application are running on the hosts, that updates were pulled and that systems are running the latest Antivirus signature files.

The answer is one word. Centralization.

In the case of using several mechanisms and backend application to verify host compliance with the organization unique security baseline, one will need to go to each of this tools, fetch the data, consolidate and process it. An example of this situation might be an organization which runs Microsoft Windows based systems with McAfee AntiVirus and ISS BlackIce would need to consolidate the data from McAfee's ePolicy orchestrator, Microsoft's Software Update Service and ISS ICECap Manager.

The expected ability from a compliance monitoring application will therefore be to be able to retrieve the security baseline information (that will be needed to translated in order for the compliance monitoring application to understand it) and scan the organization hosts for compliance with that baseline.

Scanning the hosts can be done using some scripting language or operating system management tools that can collect the various data needed to do this compliance monitoring. Since the compliance monitoring application will also need to support all the current means to secure systems (like software updates, Antivirus applications, personal firewalls) as well as future ones, it will hold templates for looking for known security application, but will also have the ability to look for different operating systems properties that can be used to scan security application and configuration change fingerprints such as: checking for file existence, different file properties, specific processes, registry entries, services, daemons and so forth.

Implementing security measures in an organization is only one side of the coin, an organization can deploy security patches regularly, install antivirus engines and the latest engine and signature files .As long as a mechanism is implemented to MAKE SURE that the user is constantly using these measures and was indeed installed with all the necessary updates (either if the culprit was a damaged software package or a user who doesn't really like the idea of such tools installed on his machine), the environment is not really secured.

4. Generic model for compliance monitoring application

At this point, the company knows what to look for in a compliance monitoring solution.
Now, let's look at a generic model for such application.

A compliance monitoring application will consist of a collector, a management console and a database that stores all the compliance data as well as the security baseline[6].

4.1. The collectors. The collector is the object that exists on the host that will be audited for compliance with the company security policy.

There are two types of collectors :

- Agent based – this requires a dedicated collector agent to be installed on any of the monitored platforms. This agent is usually a part of the code that was crafted specifically for the purpose of doing compliance audits. It can be in the form of a service in Windows based systems or a Daemon in Unix based system. Both will facilitate a process on the system that will always be running and doing its job once called for duty.

- Agent-less – In this configuration there is no reliance on any custom processes to run on the platform. The management console will have the domain or local logins in order to gain access to the monitored platform. That way the compliance monitoring application can look remotely for the files properties or registry entries.

  Note that although there is no agent on the hosts, some services must be started on the endpoint operating systems in order to allow the monitoring. Some examples are the Remote procedure call (RPC) service, Remote Registry service and the Windows Management Service (WMI). All of these services and others are used to collect data and check for the compliance markers[7].

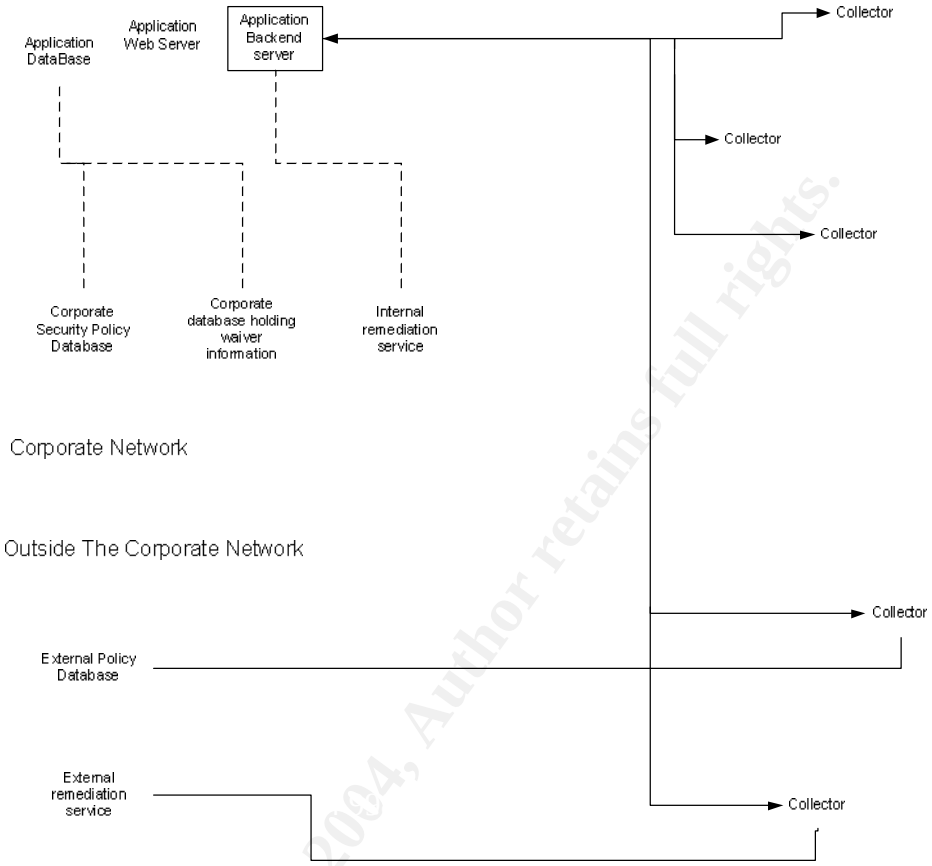

Image 2: Generic model of compliance monitoring application. Objects drawn with dotted line denote an optional object connected to the application

4.2. Database – The database is where all the collectable data is stored. The exact implementation of the database side in a compliance monitoring application will vary according to the implementation. It can be a very simple database with that will store only daily scanning results and will allow only few connections by the application administrators or it can be a very robust database running on a beefy hardware since it will need to store tens of thousands of scan results and support a very complex reporting ability.

4.3. Management console – the backend application that is usually also implemented with a web front-end.
A typical compliance monitoring management application will consist of an interface to allow feeding the security baseline needed to be monitored, an option of grouping the monitored systems by certain properties, a scheduler and set of reports.

5. The key features of good compliance monitoring solution

5.1. Scalability

A compliance monitoring solution must be one that will support the on going business of security. The same proverb – "This is not a project…this is an on going business" – that apply to many aspects of security systems and processes, apply also to a compliance monitoring solution.
It should be scalable enough to handle more systems, more operating systems, more users, looking for more security specifications and ensuring long term support. All this will ensure a compliance monitoring solution that will serve the organization for a longer period in the rapidly changing business of security[2].

A check will need to be made if the compliance monitoring application can handle the size of the organization it suppose to work in.
An important factor influencing the application's reliability is the scope of systems being monitored. A proper design should opt to run the compliance scan all the organization systems[8]. For this to happen it will need to be verified that the agent, management console and database behind are capable of handling the number of systems and users in the organization and will address any possible increase in this numbers.

The frequency of the compliance scans and the required archiving options are also factors in the application robustness.

5.2. Mapping of the current security baseline markers and looking for future needs

To be sure that the selected compliance monitoring application will be capable of scanning the current organization security baseline and also have the ability to scan for future specifications, two lists must be composed. One is the current security baseline markers list being used in the organization, and the second is a generic list of markers with the dependency of the specific operating systems.

It is very important to compose such lists because this will eliminate the possibility that one day the compliance monitoring application will be facing a security baseline that it cannot audit and check for compliance.

The following is an example of security baseline markers:
Assuming that an organization have chosen to use McAfee VirusScan Enterprise 7.0 for it's windows based system virus protection, one of

the items in the security baseline could indicate that each system must run this VirusScan anti-Virus and the scan engine must be version 4.3.2.0 or greater.
The security marker description would have to be "McAfee VirusScan Enterprise 7.0 scan engine version". The compliance monitoring application would then find that marker by looking for a specific registry entry, the status of a service (like "McShield") or any other method that may be proposed by the application templates or customized by the user.

An example for security markers can be seen in Microsoft *mssecure.xml* file which is being used in their security baseline analyzer. It contains information about each Windows system patch, such as the target operating system version and service pack level, corresponding Microsoft Knowledge Base article and security bulletin reference number, affected product and service pack IDs, registry key to be created, file version, checksum, location, and reboot requirement.[15]

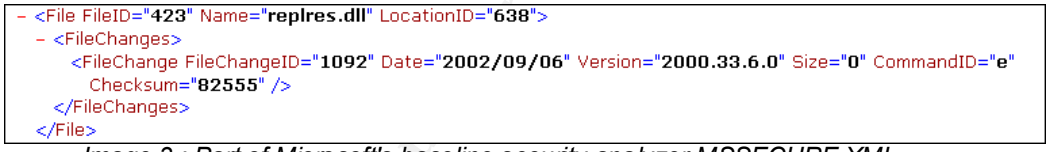

Image 3 : Part of Microsoft's baseline security analyzer MSSECURE.XML, the configuration file that hold the baseline security markers.

Another approach for defining security markers would be to create a list of a more generic markers like "Being able to read the scan engine version of all the Antivirus products currently on the market" or "Being able to read the file version of ANY file on the computer system".

An example for the generic security markers is the list below for Windows based systems:

- File existence
- File version
- File size
- File creation date
- Registry entries in all the registry hives
- Services state (Start/Stop/Disabled)
- Service startup type

5.3. Reporting

A compliance monitoring solution that supports grouping of several

endpoints according to certain properties (Department, Domain, and geographical location) will allow easy consolidation of the compliance information, while in the same time given the flexibility to run reports only for desired subset and asses the security risk of specific groups within the organization[9].

The reports generated from the compliance monitoring application should give the highest resolution and information desired: user accounts, access controls, patches and service packs level.

These reports also should provide multilevel breakouts. the same report that goes to the system administrators cannot go to the management staff.

A nice feature is also support for Ad-Hoc queries. This will help determine the state of systems within the company in a case of a major virus outbreak or if a severe vulnerability is catching the headlines - compliance status is needed ASAP.

The reporting module should sport a nice and easy interface to allow building customized reports.

5.4. Scheduling

Compliance monitoring, as the name implies is about monitoring. Continuously monitoring. Keeping a continuous stream of compliance information is in most cases not a very practical idea because of the impact it can have on the network and the host being audited.

The solution is to decide on the organization desired audit frequency and see if the compliance monitoring application can handle it. Nowadays when 0-day exploits are becoming more common the compliance data should be updated at least once on a daily basis[8]. That way a current picture of where the security holes in the organization will be delineated. This will enable the security personnel making quick decisions about next steps, whether it will be another "round of deployment" to try and get these hosts patched against the exploitation or even disconnect them from the company network connection until they are properly patched and secured according to the security policy.

5.5. Scoring and Metrics

Security metrics and appropriate scoring method is critical to understand the security status of an organization[10].

The raw output of a compliance monitoring application is the status of the monitored hosts against the security baseline as defined.

This is just a long Boolean list that looks like "Compliant with item x of the security baseline" with an answer of "yes or no".

A detailed report is an asset to the system administrators who need to know how to better secure their systems. This is also being used by the remediation component, which needs to know how to guide the end user to the specific location where he/she can find the document that will explain how to fix the specific security issues.

However, a report like that will be practically of no use when presented to your organization management staff or even to the department manager who need to quickly review his/her department security assessment and act accordingly. We cannot expect the manager to know which host is used by every employee in his/her department and cut and past the relevant lines.

For that we will need our compliance monitoring application to be able to rate each security issue and process it into a concise scorecard. The score can be in the range of 1-10 and it can be color coded (red, yellow, green) or it can be a short descriptive text[11,12].

Rating and giving the total score to a system can vary and can be as simple as giving the percentage of fixed security issues from the security baseline or it can be rather complicated by weighting other factors into the formula. A list of this factor to weight can be :

- Original vendor severity level
  Taking for example Microsoft's way of giving severity rating to their application patches, ranking for low through critical, this can add or decrease to the total score.

- Internal risk assessment
  A critical rated security patch for Outlook Express as rated by Microsoft, might get a lower severity rating in your organization if your organization is using Office Outlook and you know that chance are that not many users are using Outlook Express.

- Time since the start of deployment for the fix
  The time that elapsed since you started deploying a fix for specific vulnerability, with the consideration of the previous factors, may also influence the score for a system security. A system that is not protected yet against a critical rated vulnerability for over a month is most probably to take the "Red" zone of your compliance monitoring report – you must catch'em first !

- Importance of the business of the group to the organization

  Viewing your organization with all the different divisions, departments and groups; one can then rate their importance of their activity to the business of your organization.

Securing your development labs, finance department workstation and the servers storing your HR data is more important then securing your training rooms PCs and the public PCs that you have for the general use of contractors and visitors. Of course, any computer can be the start of your next virus crisis, but this division can still be used for your security compliance score, putting your critical resources first and lowering the total score for your engineering department if they have few machines that are still not patched against a critical vulnerability.

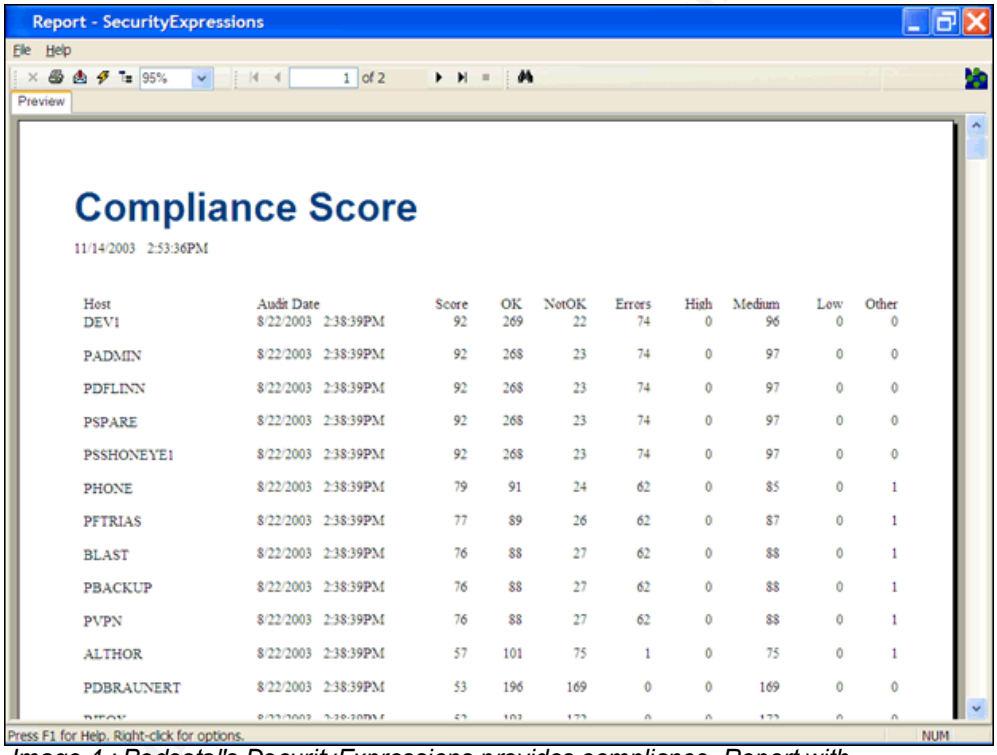

Image 4 : Pedestal's DecurityExpressions provides compliance Report with weighted average score

5.6. Easy maintenance

Ensure data entry is done easily and does not require high technical skills. although a compliance check can be easy as checking a registry key it can also be a very tedious checking for a very complex combination of file versions, file existence all mixed with logical operands

5.7. Interfaces

Like shown in the diagram of the generic compliance scanning application, the compliance monitoring application will need to interface with other applications dependent on the specific security management architecture.

these interfaces can be with:

- The database that holds the organization security baseline
- An application that holds waiver information for certain groups or users.
- Remediation resources

All the components mentioned above can reside in the organizational network but also can reside outside to support security management of road-warriors and telecommuters.

It needs to be checked in the design or with the vendor that is chosen to implement the compliance monitoring solution that these components can interface and work together in total harmony. Ideally there will be a well maintained security baseline database that can feed all the information needed to the compliance scanning application that can then point users to other resource in order to remediate their systems.

5.8. Cross platforms

Most organization have heterogeneous networks, while the most popular are Windows platform and some Unix or Linux flavors OS, it needs to be checked if there are also system like AIX, OS/390, AS/400 or even VMS . The more comprehensive your compliance monitoring application will be, less work will remain for system administrators and the compliance result will be much more accurate.

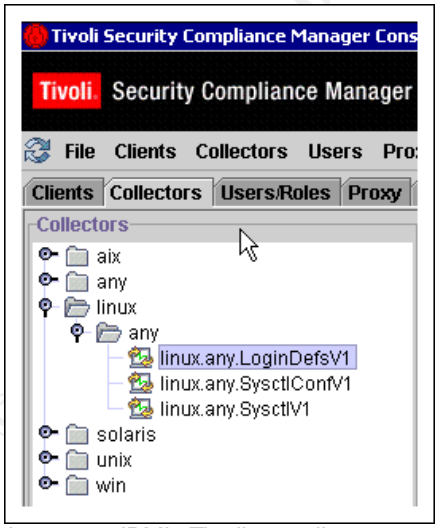

Image 5 : IBM's Tivoli compliance manager support multiple operating systems within the same management console

5.9. Agent or Agent-Less ?

As described above, in section 4, the collector of the compliance

monitoring application can be implemented in two main ways: as an agent or agent-less.

Each option has its own advantages and disadvantages that should be considered.

Agent - The agent must be installed on the client machine. The deployment should be lightweight and non disruptive for the user. Lightweight deployment will allow also installation over slow network connection.

An agent can do some security offline-monitoring as well which is advantage since it is able to support remote hosts that are not directly attached to your network, such as remote users using VPN or sales and marketing people that are on the road very frequently . This way the agent can send back the result when the user is back on a faster connection or even send the user for remediation on external networks.
Additional advantage of an agent is the ability to interact with the user, run local scripts or give clear instructions to the users in order to remediate their machine[6,14].

Using the agent-less approach for the collector is the easiest one to deploy. The compliance-monitoring application will create some kind of a database that will store user account and passwords for the targeted endpoints or use administrative account or root privileges to scan the endpoints.
To do compliance monitoring without using an agent will require the endpoint to be on the network so the management console can connect to the endpoints and send back the data. This usually also takes more of the network bandwidth [13].

5.10. Invisible monitors

Compliance, being done regularly, should have a minimum interaction with the users and should not disrupt their work. No matter if your compliance monitoring application is using the agent or the agent-less approach it should take minimum CPU and memory resource from the system being monitored. This should be considered when reviewing the systems that need to be monitored - can it run on all the systems?. If the compliance monitoring application need to interface with the users, for example if the application can point the user to a remediation resource, ensure that the interface is clear and comprehensive and can also be turned off to some groups in case they choose not to interact with the system or if the users privileges

does not allow them to install fixes and patches.

5.11. Modularity

Organizations are implementing different processes and applications to deploy patches and updates. If the deployment mechanism is not part of the specific compliance-monitoring solution, it needs to be able to interface with the deployment application. One may of course choose to have a turn-key solution in which the compliance monitoring application will be just one component in a system that does deployment and enforcement as well. Still, some non-standard endpoints may use other deployment mechanism and the ability to interface with other application might prove itself useful.

5.12. Templates and update service

Some vendors are offering a support model for their compliance monitoring solution that provide templates, information and fingerprint update for newly discovered vulnerabilities. Such a service may save resource, time and offer more accuracy while reducing the load from the data-entry process to the compliance monitoring management console

6. Conclusion

As shown in this document a good compliance monitoring application will give a data which is reliable, comprehensive and current.
checking the organization computing resource for compliance with it's security policy is an ongoing process that should happen daily as part of the organization security management, but the quality of the ongoing audit for compliance will be most visible when a 0-day exploit will hit and the fate of the organization will heavily rely on the reports that will be produced from the compliance monitoring application.

References:

[1] Sorcha Canava, An Information Security Policy Development Guide for Large Companies
www.giac.org/practical/GSEC/Sorcha_Canavan_GSEC.pdf
(November 18th, 2003)

[2] netiQ White Paper - Proactive Security Policy Enforcement: A Practical Approach
http://download.netiq.com/CMS/WHITEPAPER/NetIQ_WP_ProactivePolicyEnforcement.pdf
(Septemeber, 2003)

[3] Australian CERT recommendations, Site Security Policy Development
http://secinf.net/info/policy/auscert.html
(October 16, 2002)

[4] NIST-National Institute of Standards and Technology, An introduction to computer security: The NIST handbook
csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
(February, 1996)

[5] Jennifer L. Bayuk, Price Waterhouse, LLP - Security Through Process Management
http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper015/bayuk.pdf
(October, 1996)

[6] Jaikumar Vijayan - Extended Enforcement
http://www.computerworld.com/printthis/2004/0,4814,92943,00.html
(MAY 10, 2004)

[7] Intel Information Technology White Paper - Managing PC Security Compliance
http://www.intel.com/business/bss/infrastructure/security/pc_compliance.htm
(October, 2003)

[8] Symantec, ARTICLE ID: 3856 - Policy Compliance and Your Business
http://enterprisesecurity.symantec.com/article.cfm?articleid=3856&EID=0
(MAY 18, 2004)

[9] Eric Ogren, The Yankee Group - Best Practices for Vulnerability Management
http://www.yankeegroup.com/public/home/daily_viewpoint.jsp?ID=11447
(Copyright 1997-2002)

[10] Michael Foster- Selecting Patch Management Software
http://www.giac.org/practical/GSEC/Michael_Foster_GSEC.pdf
(January 27, 2004)

[11] John Desmond - Pedestal Adds Security Benchmark Score to Audit Software
http://www.enterpriseitplanet.com/security/news/article.php/3291401
(December 19, 2003)

[12] Tim McCollum - Security Benchmark Tools
http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=458
(June 15, 2002)

[13] Chad Robinson, Robert Frances Group - Collecting Effective Security Metrics
http://www.csoonline.com/analyst/report2412.html
(March 16, 2004)

[14] Michael Rasmussen, Forrester® - Demand for Endpoint Security Growing
http://www.csoonline.com/analyst/report2170.html
(January 29, 2004)

[15] Marcin Policht, ServerWatch ,Windows Patch Management, Introduction
http://www.serverwatch.com/tutorials/article.php/3299831
(January 15, 2004)

Vendors:

1. ConfigureSoft ECM (enterprise Configuration Manager)
   http://www.configuresoft.com/roi_compliance.htm

2. F-Secure Policy Manager
   http://www.f-secure.com/products/policy-man/index.shtml
   http://www.f-secure.com/products/policy-man/screenshots/

3. Cisco Trust Agent -
   http://www.cisco.com/en/US/products/ps5923/index.html

4. NetIQA security manager
   http://www.netiq.com/products/sm/default.asp

5. Pedestral software Securityexpression
   http://www.pedestalsoftware.com/

6. Polivec 3
   http://www.polivec.com/polivec3.html

7. Symantec Enterprise Security Manager
   http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=45&PID=11409114&EID=0

8. ENDFORCE Enterprise™ – Applied Endpoint Compliance Enforcement
   http://www.endforce.com/product.htm

9. IBM Tivoli Security Compliance Manager

   http://www-306.ibm.com/software/tivoli/library/demos/sec-comp-mgr.html

   http://publib.boulder.ibm.com/tividd/td/ITJCOL/SC32-1487-00/en_US/HTML/jac_user_guide16.htm

   http://demos.dfw.ibm.com/Recorded/Streamed/e-business/2004/IBM_Demo_Tivoli_Security_Compliance_Manager-May04.html

10. iPass Policy Orchestration
    http://www.ipass.com/platform/platform_policyorch.html

A compliance monitoring application comparison:

Mike Fratto - Policy Enforcers
http://www.networkcomputing.com/shared/printArticle.jhtml?article=/1410/1410f2full.html&pub=nwc
(May 29, 2003)

* Designated trademarks and brands are the property of their respective owners.