

Overview

One of the leading causes of security breaches and loss of data is improperly configured systems. Achieving and maintaining conformity across multiple systems challenges even the most technically adept and process-focused organizations. Even more complex is the ongoing validation that ensures that carefully-tuned security controls remain unchanged. Symantec solutions support an organization's security processes through the implementation of sound security configuration baselines, proactive evaluation, and comprehensive reporting.

Benefits

- Establish baseline configurations from best practices templates, including CIS, NIST, SANS, and others
- Evaluate IT controls against Sarbanes-Oxley, PCI DSS, HIPAA, FISMA, ISO 27001, and their regulation requirements
- Rapidly identify systems that deviate from established baselines
- Quickly remediate issues within ITIL-compliant change processes
- Assess security status through interactive reporting
- Monitor the entire enterprise with support for Windows, Linux, and UNIX

Problem Discovery Through Automation

Effective security configuration solutions empower IT organizations to implement a comprehensive security practice. As a result, organizations can implement documented audit and change processes that discover and correct lapses in standards and procedures. Discovery of problems is achieved with automated assessments that provide consistent analysis without impacting staff productivity, while integrated workflow processes ensure closed loop verification that standards are upheld. The ability to continually manage security configurations from definition, evaluation, remediation through monitoring is what distinguishes Symantec solutions from other solutions.

Build Effective Configuration Baselines

The first step to proactive security configuration management is to define effective baseline policies. However, developing these baselines can be a time-consuming, difficult task that requires extensive expertise in configuration management. Altiris solutions from Symantec simplify the process with industry best practices templates that can be implemented directly or customized to meet your needs. Altiris® SecurityExpressions™ software also supports homegrown configuration policies. Both methodologies accelerate deployment while ensuring rigorous best practices protection. The resulting policies can be tailored and published to document administrative controls.

Quickly Identify Non-compliant Systems

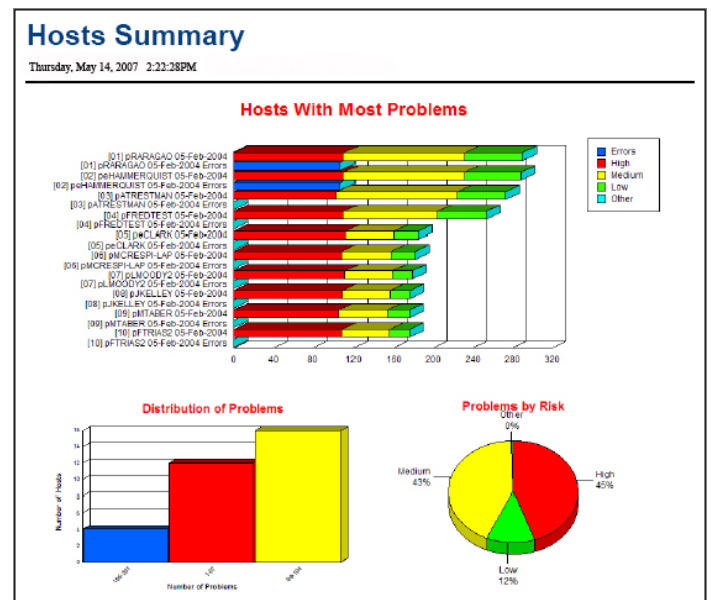
Symantec solutions allows IT and security personnel to conduct real-time audits. Altiris technology from Symantec can accurately and quickly compare the system's configurations against the company's existing policy. This process allows IT managers to conduct comprehensive audits on a frequent basis, plan and execute remediation, and re-evaluate compliance with minimal effort. In this manner, any security issues can be quickly identified and addressed. Companies can validate compliance with automated security audits rather than discover too late that vulnerabilities exist.

Tackle Issues with Closed-loop Remediation

Integration with Altiris® Helpdesk Solution™ software and Remedy, including extensibility to other service desk systems, enables organizations to plan and remediate systems while tracking configuration changes against ITIL-compliant processes. SecurityExpressions can automatically open an incident based on the audit results. IT administrators can then quickly remediate noncompliant systems using SecurityExpressions' built-in tools or integration with other Altiris management solutions from Symantec such as patch management or software delivery. Once the remediation step is complete, a secondary audit validates the fix and the incident can be closed. Closed-loop remediation improves IT change control processes without disrupting system availability.

Continually Monitor Security Status

Assessing system security postures requires the ability to not only evaluate the system, but also the ability to easily visualize the results and assess progress. SecurityExpressions provides concise reporting that summarizes the results of any audit, as well as detailed reporting that provides all of the information necessary to remediate any vulnerabilities and misconfigurations. Access to reports, including trend and noncompliance reports, allows organizations to plan remediation activities and evaluate risk-based compliance. Organizations can even weigh each rule to produce relative risk analysis, apply asset classification to weight importance, and review roll-up scores for an entire audit.



SecurityExpressions includes a comprehensive reporting function that allows you to compile dozens of reports such as trend, summary, noncompliance, and detail reports.

Detect and Evaluate Mobile Systems

Mobile systems are infrequently connected to the local network; as a result they are often missed during routine audits. Because these systems also have infrequent communication with management systems, they are more at risk for failing to comply with configuration standards. SecurityExpressions includes an optional add-on, Audit-on-Connect, to ensure that mobile systems can be audited as they connect to the network rather than on a fixed schedule, so systems that are missed in a scheduled audit can be picked up the next time they connect.

Supports Agentless and/or Agent-based Options

SecurityExpressions offers both an agentless and an agent-based option that can be mixed and matched as required across all Windows, UNIX and Linux desktops, notebooks, and servers. The included agent does not require administrative credentials and is a perfect solution for auditing servers. SecurityExpressions also has an agentless approach to reach tens of thousands of systems, effective for auditing local or remote desktops.

System Requirements

Console Requirements

- Memory—256 MB RAM (512 MB if using scheduling service)
- Minimum disk space—500 MB
- Browser—Internet Explorer 5.0 or later

Optional Server Requirements

- Memory—512 MB RAM
- Minimum disk space—500 MB
- ODBC Database—SQL Server 2000 or 2005, SQL Server Express
- Services—IIS 5.0 or later; Internet Explorer 5.0 or later to access

Operating Systems Supported

- Console—Windows Server 2000, 2003 (32- and 64-bit), XP
- Optional Server—Windows Server 2000 or Windows 2003 (32- and 64-bit)

Audit and Compliance Targets

- Operating systems—
 - Windows NT 4 (agentless only)/2000/2003 (32- and 64-bit)/2008 (scheduled to be supported summer 2008)/XP/Vista (32- and 64-bit)
 - Solaris 8 (SPARC), 9 (SPARC), 10 (SPARC and x86)
 - SUSE Linux 8, 9, 10
 - Red Hat Linux 8, 9, AS3, Enterprise 4.3
 - HP-UX 11, 11i
 - AIX 5.1, 5.2, 5.3

System Reach

- Agents on any or all systems
- Agentless on any or all systems
- Distributed proxy for remote sites

More information

Visit our Web site

<http://enterprise.symantec.com>

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our Web site.

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help businesses and consumers secure and manage their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

20330 Stevens Creek Blvd.

Cupertino, CA 95014 USA

+1 (408) 517 8000

1 (800) 721 3934

www.symantec.com

Confidence in a connected world.

