SECURITY ANALYSIS
SOLUTION

Assess and Remediate Your Security Compliance

ENDPOINT PRIVILEGED ACCESS SECURITY SUITE

Ready to secure passwords, protect endpoints, and control access?

Our Endpoint Privileged Access Security Suite consists of our flagship products:

- Secret Server
- Privilege Manager for Windows
- Privilege Manager for UNIX

Strengthen your security posture by protecting the two primary vulnerabilities in nearly every databreach: Endpoints and Privileged Accounts.

Continuous Monitoring and Remediation

Thycotic Security Analysis Solution software identifies security configuration issues using the Security Content Automation Protocol (SCAP). SCAP checklists can be imported from multiple sources, measured, and remediated with change auditing.

> **A default installation of Windows 7 is less than 40% compliant to industry recommended security standards.**

ASSESS AND SCORE SECURITY CONFIGURATION USING OPEN STANDARDS

Operations teams face the daunting challenge of parsing through security configuration assessment reports and trying to address a never ending list of security configuration issues and vulnerabilities.

Security Analysis Solution leverages industry standards such as the Security Configuration Automation Protocol and Open Vulnerability Assessment Language to assess and score the configuration state of machines. Security profiles are easily downloaded from the United States National Institute of Standards or imported from a file. Once downloaded or imported, these profiles can be edited and assessed for compliance.

CONFIGURE PREDEFINED OR CUSTOMIZABLE REMEDIATION ACTIONS

Traditional vulnerability and compliance assessment results in the time-consuming process of interpreting the results, applying a remediation, and waiting for the next scan to measure success. With Security Analysis Solution, the challenge of remediation is simplified.

- Predefined remediation actions for the rules in industry standard checklists
- Customized remediation actions can be defined using scripts and built-in tasks
- When rules are found to be out of compliance in an assessment, the remediation job is created and ready to execute pending approval

thycotic

1101 17th Street NW Suite 1102
Washington DC 20036
DC | LONDON | SYDNEY

p: +1 202-802-9399
t: @thycotic
www.thycotic.com

EXTEND YOUR ALTIRIS & SYMANTEC INVESTMENT

Thycotic solutions are natively integrated into the Symantec Management Platform and leverage your investment in the platform. This reduces your overall cost and increases ROI.

REVIEW ASSESSMENTS AND APPROVE REMEDIATION

Security Analysis Solution uses policies to target a set of computers and measure their compliance to a security profile. Assessments will provide a score by computer with details of the compliance for each rule in a security profile. Policies will measure the overall compliance for the targeted computers with historic trends.

If policies are defined to include remediation, a job is created for each computer to correct settings according to the associated remediation actions. Remediation jobs require approval making it easy to incorporate into a change control process. Remediation jobs can be run for an individual computer or for multiple computers in a single step.

CONFIRMING REMEDIATION

Closed loop remediation ensures that the actions taken to fix a problem were confirmed. Upon completion of a remediation job, results are generated to validate the remediation steps completed successfully. Future security assessments will indicate an improved security configuration score and provide ongoing monitoring for compliance.

thycotic

1101 17th Street NW Suite 1102
Washington DC 20036
DC | LONDON | SYDNEY

p: +1 202-802-9399
t: @thycotic
www.thycotic.com