Hardening the Soft Middle: Securing your IT Infrastructure through Configuration Baselining

A White Paper

By Brian McCormack

Hardening the Soft Middle: Securing your IT Infrastructure through Configuration Baselining

By Brian McCormack

The IT infrastructure is a corporation's most valuable asset, delivering competitive advantages, processing the bulk of business transactions, and storing confidential information on all areas of the company, including financial data, customer and supplier databases, engineering schedules, business plans, human resource records, and email.

All this information is online. And it's all vulnerable. It must be protected constantly and thoroughly without interrupting business.

Failure to do so can result in staggering losses, both tangible and intangible. The Computer Security Institute, for example, determined that the theft of proprietary information cost companies over $150 million in 2001. Viruses cost them another $45 million, while Internet abuse by insiders cost $35 million. Add to that the intangible, such as loss of competitive advantage and customer trust and it's clear: secure your data or be doomed.

Enterprises invest heavily in infrastructure security, often taking a medieval fortress approach: keep the hackers and bad guys out. More often than not, the enemy is within. The Gartner Group forecasts that by 2004, 90 percent of all security breeches will originate inside companies.

And even when employees are not stealing secrets, they may be compromising security by flouting IT operating procedures. In one survey, the Gartner Group found that 56 percent of companies had suffered an abuse of computer access controls, and that 78 percent had employees installing or using unauthorized software.

All such activity occurs in what we call the "soft middle," the sections of the enterprise between the firewalls. Particularly vulnerable in this area "inside the perimeter" are servers, switches, routers, and workstations. Common vulnerabilities include:

- Default configurations that are left unchanged
- Default passwords that are left unchanged
- Configuration of unnecessary services
- Latest security patches are not installed

How do companies let such security lapses stand? IT staff is often faced with a lack of time, inadequate methods of documentation, and an overall lack of consistency in creating and monitoring configuration standards.

Hardening the Soft Middle—A Three-Step Approach

Step 1. Creating "security templates"

The first step is to develop and use a **Security Template**. Such a template can help enforce best practices, reduce common vulnerabilities, define and enforce access rules, and facilitate continuous IT auditing.

A typical security template for a server might include user access and permissions, the disabling of unnecessary defaults, the placement of the latest securities patches, and the monitoring of shared drives. A template for a router would include provisions to address the network's interactive access and the known vulnerabilities of HTTP services.

Resources for creating a Security Template can be found on several Internet sites, including:

CERT (Computer Emergency Response Team) Coordination Center:
www.cert.org

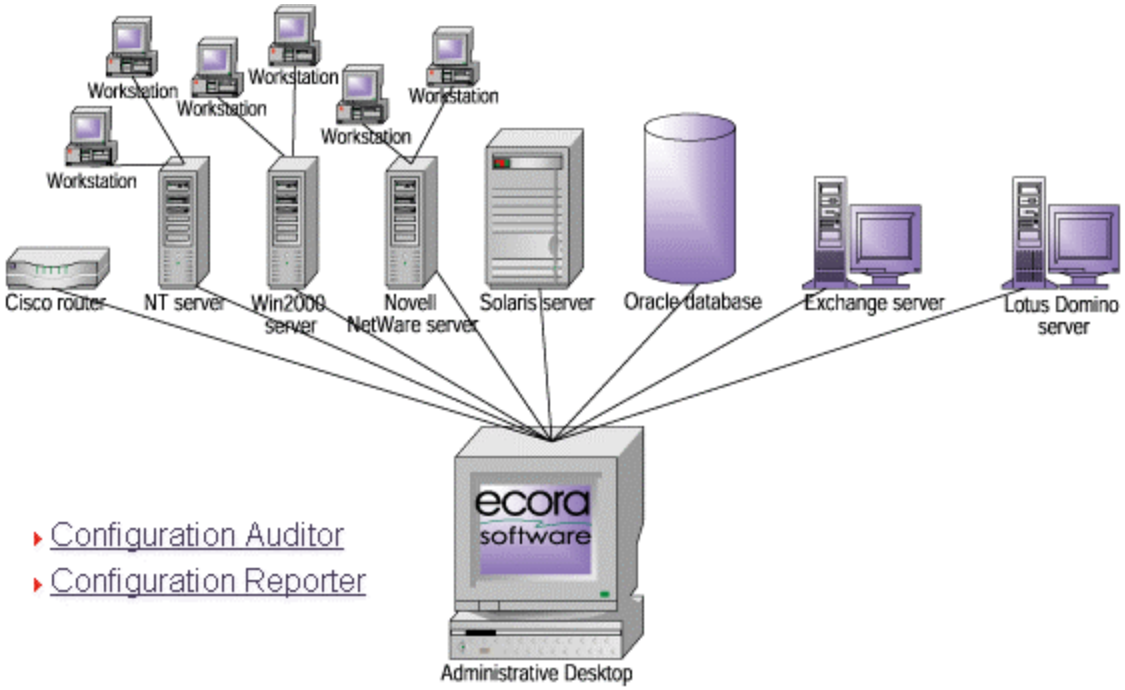
The SANS (Systems Administration, Networking, and Security) Institute:
www.sans.org/newlook/resources/

Vendor websites, including Cisco Systems:
www.cisco.com/pcgi-bin/front.x/csec/csecHome.pl

Step 2: Selecting the right automated solution

The limitation of security templates is they become just static documents without the means to incorporate them into some type of automated solution that can regularly monitor an infrastructure. To manually configure, baseline, and monitor every server, router, and workstation in an enterprise would require armies of people—resources most companies do no have or cannot spare.

Since various automated solutions for information collection and monitoring exist, **selecting the right tool** is the second step towards ensuring security. When incorporated into an automated solution such as Ecora's Configuration Auditor, the security templates serve as the basis for the error-proof maintenance of all the configuration settings in an enterprise.



At user-defined points in time, Configuration Auditor can track over 100,000 changes in an infrastructure: network devices, servers, workstations, databases, and applications. An automated solution can also track configuration changes that impact security, such as access control lists, system user groups, roles and privileges, and router and switch settings.

So with general security templates for specific types of IT devices fully developed, and an automated system in place to monitor the infrastructure, the pieces are in place to create a corporate “gold standard” for security and performance—the baseline report.

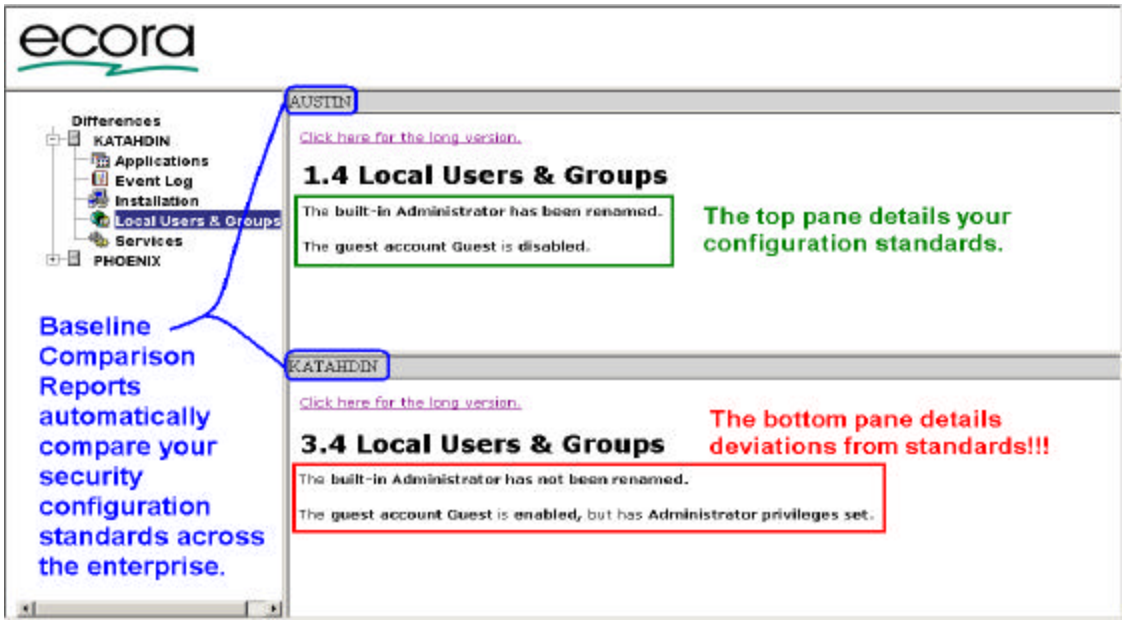
Step 3: Creating a “Cycle of Control”

Once security templates are integrated into an automated solution, the final step towards total security lies in creating a “cycle of control,” in which performance baselines are established, reports are run to detect instances of noncompliance, settings are reconfigured, if need be, and templates updated—all as part of a regularly scheduled security cycle.

Such a Cycle of Control has three phases:

1. Running Baseline Reports
2. Updating Configurations as needed
3. Verifying changes and updating security templates

Baselining is a way to set and enforce standards. A baseline report is divided into two panes. Reports can be scheduled to run to compare like devices against security templates. The top pane shows a configuration standard. The bottom pane details deviations.



With baseline reports, a routine can be established for doing periodic sweeps of the IT infrastructure to verify that security holes have been plugged, that there is compliance with company policies and best practices, and that security patches have been installed.

This straightforward cycle is an efficient way to harden the soft middle of security, especially in today's environments where networks are in a constant state of change due to mergers and acquisitions, employee turnover, and the endless adding, deleting, and modifying of user accounts and permissions.

In summary, most security breeches occur inside the firewall, in an infrastructure's "soft middle." The best way to tighten up this middle is by developing security templates for each type of network device and using documentation and baseline report features on automated solutions to create a "cycle of control" for all key security settings.

For security assessments, automated products such as Ecora provide continuous audits and vigilant tracking of hundreds of security related configuration settings, detailed configuration reports across multiple platforms, and change reports on one IT element or groups of elements.

Brian McCormack (bmccormack@ecora.com) is a Product Manager and baselining expert at Ecora Software.